SUSE Linux

10.1 www.novell.com

02/28/2006 Referencia

Referencia

Autores: Jörg Arndt, Stefan Behlert, Frank Bodammer, James Branam, Volker Buzek, Klara Cihlarova, Stefan Dirsch, Olaf Donjak, Roman Drahtmüller, Thorsten Dubiel, Torsten Duwe, Thomas Fehr, Stefan Fent, Werner Fink, Jakub Friedl, Kurt Garloff, Joachim Gleißner, Carsten Groß, Andreas Grünbacher, Berthold Gunreben, Franz Hassels, Andreas Jaeger, Jana Jaeger, Klaus Kämpf, Andi Kleen, Hubert Mantel, Lars Marowsky-Bree, Chris Mason, Johannes Meixner, Lars Müller, Matthias Nagorni, Anas Nashif, Siegfried Olschner, Edith Parzefall, Peter Pöml, Thomas Renninger, Hannes Reinecke, Scott Rhoades, Thomas Rölz, Heiko Rommel, Tanja Roth, Marcus Schäfer, Thomas Schraitle, Klaus Singvogel, Frank Sundermeyer, Elisabeth Tobiasson, Hendrik Vogelsang, Klaus G. Wagner, Rebecca Walter, Christian Zoz

Esta publicación es propiedad intelectual de Novell Inc.

Su contenido puede duplicarse, ya sea en su totalidad o en parte, siempre que haya un símbolo de copyright bien visible en cada copia.

Toda la información recogida en esta publicación se ha compilado prestando toda la atención posible al más mínimo detalle. Sin embargo, esto no garantiza una precisión total. Ni SUSE LINUX GmbH, los autores ni los traductores serán responsables de los posibles errores o las consecuencias que de ellos pudieran derivarse.

Novell, el logotipo de Novell, el logotipo N y SUSE son marcas comerciales registradas de Novell, Inc. en los Estados Unidos y en otros países. * Linux es una marca registrada de Linus Torvalds. El resto de marcas comerciales de otros fabricantes pertenecen a sus propietarios respectivos.

Si tiene alguna sugerencia o comentario, diríjalos a `documentation@suse.de`.

Tabla de contenidos

Acerca de esta guía **xi**

Parte 1 Escenarios de implantación avanzados **15**

1 Instalación remota **17**

1.1 Situaciones de instalación para la instalación remota 17
1.2 Configuración del servidor que almacena las fuentes de la instalación . . . 27
1.3 Preparación del arranque del sistema de destino 37
1.4 Arranque del sistema de destino para la instalación 47
1.5 Monitorización del proceso de instalación 52

2 Configuración avanzada de disco **57**

2.1 Configuración de LVM 57
2.2 Configuración de RAID de software 64

3 Actualización del sistema y gestión de paquetes **71**

3.1 Actualización de SUSE Linux 71
3.2 Cambios de software de versión a versión 74
3.3 Gestor de paquetes RPM 94

Parte 2 Administración **107**

4 Seguridad en Linux **109**

4.1 Enmascaramiento y cortafuegos 109
4.2 SSH: operaciones de red seguras 121

4.3 Cifrado de particiones y archivos . . . 127
4.4 Limitación de privilegios con AppArmor . . . 130
4.5 Seguridad y confidencialidad . . . 140

5 Listas de control de acceso en Linux 155

5.1 Permisos de archivo tradicionales . . . 155
5.2 Ventajas de las ACL . . . 157
5.3 Definiciones . . . 158
5.4 Gestión de las ACL . . . 158
5.5 Compatibilidad de ACL con las aplicaciones . . . 167
5.6 Información adicional . . . 167

6 Utilidades de monitorización del sistema 169

6.1 Lista de archivos abiertos: `lsof` . . . 170
6.2 Usuarios que acceden a los archivos: `fuser` . . . 171
6.3 Propiedades del archivo: `stat` . . . 172
6.4 Dispositivos USB: `lsusb` . . . 172
6.5 Información acerca de un dispositivo SCSI: `scsiinfo` . . . 173
6.6 Procesos: `top` . . . 173
6.7 Lista de procesos: `ps` . . . 175
6.8 Árbol de procesos: `pstree` . . . 176
6.9 Usuarios y acciones `w` . . . 177
6.10 Utilización de la memoria: `free` . . . 177
6.11 Buffer de anillo del núcleo: `dmesg` . . . 177
6.12 Sistemas de archivos y su utilización: `mount`, `df` y `du` . . . 178
6.13 Sistema de archivos `/proc` . . . 179
6.14 Recursos PCI: `lspci` . . . 182
6.15 Llamadas del sistema para ejecutar un programa: `strace` . . . 183
6.16 Llamadas de la biblioteca para ejecutar un programa: `ltrace` . . . 184
6.17 Especificación de la biblioteca necesaria: `ldd` . . . 185
6.18 Información adicional acerca de los binarios ELF . . . 185
6.19 Comunicación entre procesos: `ipcs` . . . 186
6.20 Medición del tiempo con `time` . . . 186

Parte 3 Sistema 187

7 Aplicaciones de 32 bits y de 64 bits en un entorno de sistema de 64 bits 189

7.1 Asistencia sobre tiempo de ejecución . . . 189
7.2 Desarrollo de software . . . 190
7.3 Compilación de software en plataformas de doble arquitectura . . . 191

7.4 Especificaciones de núcleo 192

8 Arranque y configuración de un sistema Linux 193

8.1 Proceso de arranque de Linux 193
8.2 Proceso init 197
8.3 Configuración del sistema mediante /etc/sysconfig 206

9 Cargador de arranque 211

9.1 Selección de un cargador de arranque 212
9.2 Arranque con GRUB 212
9.3 Configuración del Cargador de arranque con YaST 222
9.4 Desinstalación del cargador de arranque de Linux 228
9.5 Creación de CD de arranque 228
9.6 Pantalla gráfica de SUSE 229
9.7 Solución de problemas 230
9.8 Información adicional 232

10 Funciones especiales de SUSE Linux 233

10.1 Información acerca de paquetes especiales de software 233
10.2 Consolas virtuales 240
10.3 Distribución del teclado 241
10.4 Ajustes de idioma y país 242

11 Funcionamiento de la impresora 247

11.1 Flujo de trabajo del sistema de impresión 249
11.2 Métodos y protocolos de conexión de impresoras 249
11.3 Instalación del software 250
11.4 Configuración de la impresora 251
11.5 Configuración para aplicaciones 257
11.6 Funciones especiales en SUSE Linux 258
11.7 Solución de problemas 264

12 Gestión dinámica de dispositivos de núcleo con udev 273

12.1 Directorio /dev 273
12.2 uevents y udev del núcleo 274
12.3 Controladores, módulos del núcleo y dispositivos 274
12.4 Arranque y configuración inicial del dispositivo 275
12.5 Depuración de los eventos udev 276
12.6 Influencia de la gestión de eventos de dispositivo del núcleo con reglas de udev 277

12.7 Denominación permanente de dispositivos . . . 277
12.8 Paquete hotplug sustituido . . . 278
12.9 Información adicional . . . 279

13 Sistemas de archivos en Linux 281

13.1 Terminología . . . 281
13.2 Sistemas de archivos de Linux principales . . . 282
13.3 Otros sistemas de archivos compatibles . . . 289
13.4 Compatibilidad con archivos grandes en Linux . . . 290
13.5 Información adicional . . . 292

14 El sistema X Window 293

14.1 Configuración de X11 con SaX2 . . . 293
14.2 Optimización de la configuración de X . . . 295
14.3 Instalación y configuración de fuentes . . . 301
14.4 OpenGL: configuración 3D . . . 307

15 FreeNX: control remoto de otro equipo 311

15.1 Procedimientos iniciales de NX . . . 311
15.2 Configuración avanzada de FreeNX . . . 314
15.3 Solución de problemas . . . 321
15.4 Información adicional . . . 323

16 Autenticación con PAM 325

16.1 Estructura de archivos de configuración PAM . . . 326
16.2 Configuración PAM para sshd . . . 328
16.3 Configuración de módulos PAM . . . 330
16.4 Información adicional . . . 332

17 Virtualización mediante Xen 335

17.1 Instalación de Xen . . . 337
17.2 Instalación de dominios . . . 338
17.3 Inicio y control de los dominios Xen con xm . . . 339
17.4 Solución de problemas . . . 340
17.5 Información adicional . . . 341

Parte 4 Servicios **343**

18 Trabajo en red básico **345**

18.1 Direcciones IP y encaminamiento 348
18.2 IPv6: Internet de la próxima generación 351
18.3 Resolución de nombres 361
18.4 Configuración de una conexión de red de con YaST 362
18.5 Gestión de conexiones de red con NetworkManager 374
18.6 Configuración manual de una conexión de red 377
18.7 smpppd como asistente de acceso telefónico 389

19 Servicios SLP en la red **393**

19.1 Registro de sus propios servicios 393
19.2 Interfaces SLP en SUSE Linux 394
19.3 Activación de SLP 395
19.4 Información adicional 395

20 Sistema de nombres de dominio (DNS) **397**

20.1 Terminología de DNS 397
20.2 Configuración con YaST 398
20.3 Inicio del servidor de nombres BIND 406
20.4 Archivo de configuración /etc/named.conf 408
20.5 Archivos de zona 412
20.6 Actualización dinámica de los datos de zona 417
20.7 Transacciones seguras 417
20.8 Seguridad DNS 419
20.9 Información adicional 419

21 Uso de NIS **421**

21.1 Configuración de los servidores NIS 421
21.2 Configuración de clientes NIS 428

22 Uso compartido de sistemas de archivos con NFS **431**

22.1 Importación de sistemas de archivos con YaST 431
22.2 Importación manual de sistemas de archivos 432
22.3 Exportación de sistemas de archivos con YaST 433
22.4 Exportación manual de sistemas de archivos 434
22.5 Información adicional 437

23 DHCP **439**

23.1 Configuración de un servidor DHCP con YaST 440
23.2 Paquetes de software DHCP 444
23.3 El servidor DHCP dhcpd 444
23.4 Información adicional 448

24 Sincronización de la hora con NTP **449**

24.1 Configuración de un cliente NTP con YaST 449
24.2 Configuración de xntp en la red 453
24.3 Configuración de un reloj local de referencia 453

25 Servicio de directorios LDAP **455**

25.1 LDAP frente a NIS 457
25.2 Estructura de un árbol de directorios de LDAP 458
25.3 Configuración del servidor con slapd.conf 461
25.4 Gestión de datos en el directorio LDAP 466
25.5 El cliente LDAP de YaST 470
25.6 Configuración de los usuarios y grupos LDAP en YaST 479
25.7 Información adicional 480

26 Servidor HTTP Apache **483**

26.1 Inicio rápido 483
26.2 Configuración de Apache 485
26.3 Inicio y detención de Apache 500
26.4 Instalación, activación y configuración de módulos 502
26.5 Puesta en funcionamiento de guiones CGI 510
26.6 Configuración de un servidor Web seguro con SSL 513
26.7 Cómo evitar problemas de seguridad 520
26.8 Solución de problemas 522
26.9 Información adicional 523

27 Sincronización de archivos **525**

27.1 Software de sincronización de datos disponible 525
27.2 Factores determinantes para seleccionar un programa 529
27.3 Introducción a Unison 533
27.4 Introducción a CVS 535
27.5 Introducción a Subversion 538
27.6 Introducción a rsync 541
27.7 Introducción a mailsync 543

28 Samba **547**

28.1 Terminología 547
28.2 Inicio y detención de Samba 549
28.3 Configuración de un servidor Samba 549
28.4 Configuración de los clientes 555
28.5 Samba como servidor de inicio de sesión 556
28.6 Información adicional 558

29 Servidor alterno Squid **559**

29.1 Algunos aspectos de los cachés alternos 560
29.2 Requisitos del sistema 562
29.3 Inicio de Squid 564
29.4 Archivo de configuración /etc/squid/squid.conf 566
29.5 Configuración de un alterno transparente 572
29.6 cachemgr.cgi 575
29.7 squidGuard 577
29.8 Generación de informes de caché con Calamaris 578
29.9 Información adicional 579

Parte 5 Movilidad **581**

30 Informática móvil con Linux **583**

30.1 Equipos portátiles 583
30.2 Hardware móvil 591
30.3 Teléfonos móviles y dispositivos PDA 592
30.4 Información adicional 593

31 PCMCIA **595**

31.1 Control de las tarjetas PCMCIA mediante pccardctl 596
31.2 Descripción detallada de PCMCIA 597
31.3 Solución de problemas 600

32 Gestión de perfiles de la configuración del sistema **605**

32.1 Terminología 606
32.2 Configuración de SCPM 606
32.3 Configuración de SCPM mediante una interfaz gráfica del usuario 607
32.4 Configuración de SCPM mediante la línea de comando 614
32.5 Solución de problemas 617
32.6 Información adicional 619

33 Gestión de energía **621**

33.1 Funciones de ahorro de energía 622
33.2 APM 623
33.3 ACPI 625
33.4 Detención del disco duro 633
33.5 Paquete powersave 634
33.6 Módulo de gestión de energía de YaST 644

34 Comunicación inalámbrica **649**

34.1 LAN inalámbrica 649
34.2 Bluetooth 661
34.3 Transmisión de datos mediante infrarrojos 673

Índice **677**

Acerca de esta guía

Este manual ofrece una descripción general de SUSE Linux. Está destinado, principalmente, a administradores de sistemas, y a personas que hacen de él un uso doméstico y que tienen conocimientos básicos de administración de sistemas. Este manual presenta una selección de aplicaciones necesarias en la vida diaria y proporciona descripciones exhaustivas de las situaciones de instalación y configuración avanzadas.

Escenarios de implantación avanzados
: Aprenda a implantar SUSE Linux en entornos complejos.

Administración
: Aprenda a incrementar la seguridad de su sistema SUSE Linux o a gestionar los controles de acceso al sistema de archivos y conozca algunas utilidades importantes para los administradores de Linux.

Sistema
: Lea una introducción de los componentes del sistema Linux y alcance una mejor comprensión de su interacción.

Servicios
: Aprenda cómo configurar varios servicios de red y de archivo que incluye SUSE Linux.

Movilidad
: Iníciese en los equipos móviles con SUSE Linux y aprenda a configurar las múltiples opciones correspondientes a los equipos inalámbricos, la gestión de alimentación y la gestión de perfiles.

1 Comentarios

Nos gustaría recibir sus comentarios o sugerencias acerca de este manual y del resto de documentación incluida en este producto. Utilice la función de comentarios del usuario, situada en la parte inferior de cada página de la documentación en línea, para escribir sus comentarios.

2 Documentación adicional

Hay más manuales disponibles sobre este producto SUSE Linux, bien en línea en `http://www.novell.com/documentation/`, bien en el sistema instalado en `/usr/share/doc/manual/`:

Guía de inicio de SUSE Linux
: Esta guía presenta el procedimiento de instalación de SUSE Linux y la utilización básica de su entorno de escritorio. Puede encontrar una versión en línea de este documento en `http://www.novell.com/documentation/suse101/`.

Guía de aplicaciones de SUSE Linux
: Esta guía proporciona una selección de las herramientas más importantes que ofrece SUSE Linux. Puede encontrar una versión en línea de este documento en `http://www.novell.com/documentation/suse101/`.

Guía de administración de Novell AppArmor 2.0
: Esta guía contiene información detallada acerca del uso de *AppArmor* en su entorno. Puede encontrar una versión en línea de este documento en `http://www.novell.com/documentation/apparmor/`.

3 Convenciones de la documentación

En este manual se utilizan las siguientes convenciones tipográficas:

- `/etc/passwd:` nombres de archivos y de directorios.
- *`espacio reservado:`* se sustituye *`espacio reservado`* por el valor real.
- `PATH`: variable de entorno PATH.
- `ls`, `--help`: comandos, opciones y parámetros.
- `usuario:` usuarios o grupos.
- Alt, Alt + F1: tecla que pulsar o combinación de teclas. Aparecen en mayúsculas, tal y como se muestran en el teclado.
- *Archivo, Archivo → Guardar como:* elementos de menú y botones.

- *Pingüinos bailarines* (capítulo Pingüinos, ↑*Referencia*): referencia a un capítulo en otro libro.

4 Acerca de la elaboración de este manual

Este manual se ha escrito en Novdoc, una sección de DocBook (consulte `http://www.docbook.org`). Los archivos XML de origen se han validado con `xmllint`, procesado con `xsltproc` y convertido a HTML con una versión personalizada de las hojas de estilo de Norman Walsh.

5 Créditos

Con su gran esfuerzo voluntario, los desarrolladores de Linux cooperan en todo el mundo para promocionar el desarrollo de Linux. Les damos las gracias a todos por su esfuerzo: esta distribución no existiría sin ellos. Asimismo, gracias a Frank Zappa y Pawar. Gracias especiales, por supuesto, a Linus Torvalds.

¡Qué disfrutéis!

Vuestro equipo de SUSE

Parte 1. Escenarios de implantación avanzados

1 Instalación remota

SUSE Linux se puede instalar de varias maneras diferentes. Además de la instalación habitual a partir de CDs o DVDs descrita en el Capítulo *Instalación mediante YaST* (↑Inicio), es posible seleccionar diversos métodos basados en red o incluso utilizar un método sin intervención física alguna para instalar SUSE Linux.

Más adelante se ofrece una introducción a cada método con dos listas de comprobación, una con los requisitos previos y otra en la que se describe el procedimiento básico. A continuación se incluyen más detalles de las técnicas utilizadas en cada situación de instalación.

NOTA

En las próximas secciones, el sistema que almacenará la nueva instalación de SUSE Linux aparece como *sistema de destino* o *destino de la instalación*. El término *fuente de la instalación* se utiliza para todas las fuentes de datos de instalación. Esto incluye medios físicos, tales como CD y DVD, y los servidores de red que distribuyan los datos de instalación en la red.

1.1 Situaciones de instalación para la instalación remota

En esta sección se describen las situaciones de instalación más habituales para la instalación remota. Para cada situación, compruebe detenidamente los requisitos previos

y siga el procedimiento indicado. Si necesita instrucciones detalladas para un paso concreto, siga los enlaces que aparecen en cada uno de ellos.

IMPORTANTE

La configuración de X Window System no forma parte del proceso de instalación remota. Cuando finalice la instalación, inicie la sesión en el sistema de destino como usuario root, escriba `telinit 3` e inicie SaX2 para configurar el hardware como se describe en la Sección 14.1, “Configuración de X11 con SaX2” (p. 293).

1.1.1 Instalación remota sencilla mediante VNC: configuración de red estática

Para este tipo de instalación, es necesario un cierto grado de acceso físico al sistema de destino con el fin de arrancarlo para la instalación. Una estación de trabajo remota controla completamente la instalación propiamente dicha y usa VNC para conectarse al programa de instalación. Es necesaria la misma intervención del usuario que en la instalación manual descrita en el Capítulo *Instalación mediante YaST* (↑Inicio).

Para este tipo de instalación, asegúrese de que se cumplen los siguientes requisitos:

- Fuente de la instalación remota: NFS, HTTP, FTP o SMB con una conexión de red en funcionamiento
- Sistema de destino con una conexión de red en funcionamiento
- Sistema de control con una conexión de red en funcionamiento y con software para la visualización de VNC o un navegador compatible con Java (Firefox, Konqueror, Internet Explorer u Opera)
- Medio de arranque físico (CD o DVD) para arrancar el sistema de destino
- Direcciones IP estáticas válidas ya asignadas a la fuente de la instalación y al sistema de control
- Dirección IP estática válida para asignar al sistema de destino

Para realizar este tipo de instalación, siga estos pasos:

1 Configure la fuente de la instalación tal y como se describe en la Sección 1.2, "Configuración del servidor que almacena las fuentes de la instalación" (p. 27).

2 Arranque el sistema de destino mediante el primer CD o DVD del kit de medios de SUSE Linux.

3 Cuando aparezca la pantalla de arranque del sistema de destino, utilice el menú de opciones de arranque para establecer las opciones de VNC apropiadas y la dirección de la fuente de la instalación. Esto se describe con más detalle en la Sección 1.4, "Arranque del sistema de destino para la instalación" (p. 47).

   El sistema de destino inicia un entorno basado en texto y ofrece la dirección de red y el número de pantalla mediante los cuales las aplicaciones para la visualización de VNC o navegadores pueden dirigirse al entorno de instalación gráfica. Las instalaciones VNC se anuncian ellas mismas en OpenSLP, y pueden encontrarse usando Konqueror en modo `service://` o `slp://`.

4 En la estación de trabajo de control, abra una aplicación para la visualización de VNC o un navegador Web y conéctese al sistema de destino como se describe en la Sección 1.5.1, "Instalación de VNC" (p. 52).

5 Realice la instalación como se describe en el Capítulo *Instalación mediante YaST* (↑Inicio).

   Es necesario volver a conectarse al sistema de destino después de reiniciarlo para la parte final de la instalación.

6 Complete la instalación.

1.1.2 Instalación remota sencilla mediante VNC: configuración de red dinámica mediante DHCP

Para este tipo de instalación, es necesario un cierto grado de acceso físico al sistema de destino con el fin de arrancarlo para la instalación. La configuración de la red se realiza mediante DHCP. Una estación de trabajo remota controla completamente la instalación propiamente dicha y usa VNC para conectarse al programa de instalación, pero es necesaria la intervención del usuario para realizar la configuración.

Para este tipo de instalación, asegúrese de que se cumplen los siguientes requisitos:

- Fuente de la instalación remota: NFS, HTTP, FTP o SMB con una conexión de red en funcionamiento
- Sistema de destino con una conexión de red en funcionamiento
- Sistema de control con una conexión de red en funcionamiento y con software para la visualización de VNC o un navegador compatible con Java (Firefox, Konqueror, Internet Explorer u Opera)
- Medio de arranque físico (CD, DVD o disco de inicio personalizado) para arrancar el sistema de destino
- Servidor DHCP en funcionamiento que suministre las direcciones IP

Para realizar este tipo de instalación, siga estos pasos:

1. Configure la fuente de la instalación tal y como se describe en la Sección 1.2, "Configuración del servidor que almacena las fuentes de la instalación" (p. 27). Escoja un servidor de red NFS, HTTP o FTP. Si la fuente de la instalación es SMB, consulte la Sección 1.2.5, "Gestión de una fuente de instalación SMB" (p. 35).

2. Arranque el sistema de destino mediante el primer CD o DVD del kit de medios de SUSE Linux.

3. Cuando aparezca la pantalla de arranque del sistema de destino, utilice el menú de opciones de arranque para establecer las opciones de VNC apropiadas y la dirección de la fuente de la instalación. Esto se describe con más detalle en la Sección 1.4, "Arranque del sistema de destino para la instalación" (p. 47).

   El sistema de destino inicia un entorno basado en texto y ofrece la dirección de red y el número de pantalla mediante los cuales las aplicaciones para la visualización de VNC o navegadores pueden dirigirse al entorno de instalación gráfica. Las instalaciones VNC se anuncian ellas mismas en OpenSLP, y pueden encontrarse usando Konqueror en modo `service://` o `slp://`.

4. En la estación de trabajo de control, abra una aplicación para la visualización de VNC o un navegador Web y conéctese al sistema de destino como se describe en la Sección 1.5.1, "Instalación de VNC" (p. 52).

5 Realice la instalación como se describe en el Capítulo *Instalación mediante YaST* (↑Inicio).

   Es necesario volver a conectarse al sistema de destino después de reiniciarlo para la parte final de la instalación.

6 Complete la instalación.

1.1.3 Instalación remota mediante VNC: arranque en PXE y Wake on LAN

Este tipo de instalación no requiere intervención física alguna. La máquina de destino se inicia y arranca de manera remota. Sólo es necesaria la intervención del usuario para la instalación propiamente dicha. Este método es adecuado para instalaciones en múltiples ubicaciones.

Para este tipo de instalación, asegúrese de que se cumplen los siguientes requisitos:

- Fuente de la instalación remota: NFS, HTTP, FTP o SMB con una conexión de red en funcionamiento
- Servidor TFTP
- Servidor DHCP en funcionamiento para su red
- Sistema de destino compatible con arranque en PXE, funcionamiento en red y Wake on LAN, enchufado y conectado a la red
- Sistema de control con una conexión de red en funcionamiento y con software para la visualización de VNC o un navegador compatible con Java (Firefox, Konqueror, Internet Explorer u Opera)

Para realizar este tipo de instalación, siga los pasos siguientes:

1 Configure la fuente de la instalación tal y como se describe en la Sección 1.2, “Configuración del servidor que almacena las fuentes de la instalación” (p. 27). Escoja un servidor de red NFS, HTTP o FTP o configure una fuente de instalación SMB como se describe en la Sección 1.2.5, “Gestión de una fuente de instalación SMB” (p. 35).

2 Configure un servidor TFTP para que almacene una imagen de arranque que pueda ser utilizada por el sistema de destino. Esto se describe en la Sección 1.3.2, “Configuración de un servidor TFTP” (p. 38).

3 Configure un servidor DHCP para que suministre direcciones IP a todas las máquinas e indique la ubicación del servidor TFTP al sistema de destino. Esto se describe en la Sección 1.3.1, “Configuración de un servidor DHCP” (p. 37).

4 Prepare el sistema de destino para arranque en PXE. Esto se describe con más detalle en la Sección 1.3.5, “Preparación del sistema de destino para arranque en PXE” (p. 45).

5 Comience el proceso de arranque del sistema de destino mediante Wake on LAN. Esto se describe en la Sección 1.3.7, “Wake on LAN” (p. 46).

6 En la estación de trabajo de control, abra una aplicación para la visualización de VNC o un navegador Web y conéctese al sistema de destino como se describe en la Sección 1.5.1, “Instalación de VNC” (p. 52).

7 Realice la instalación como se describe en el Capítulo *Instalación mediante YaST* (↑Inicio).

   Es necesario volver a conectarse al sistema de destino después de reiniciarlo para la parte final de la instalación.

8 Complete la instalación.

1.1.4 Instalación remota sencilla mediante SSH: configuración de red estática

Para este tipo de instalación es necesario un cierto grado de acceso físico al sistema de destino con el fin de arrancarlo para la instalación y de determinar la dirección IP del destino de la instalación. Una estación de trabajo remota controla completamente la instalación propiamente dicha y usa SSH para conectarse al programa de instalación. Es necesaria la misma intervención del usuario que en la instalación manual descrita en el Capítulo *Instalación mediante YaST* (↑Inicio).

Para este tipo de instalación, asegúrese de que se cumplen los siguientes requisitos:

- Fuente de la instalación remota: NFS, HTTP, FTP o SMB con una conexión de red en funcionamiento
- Sistema de destino con una conexión de red en funcionamiento
- Sistema de control con una conexión de red y software cliente para SSH en funcionamiento
- Medio de arranque físico (CD, DVD o disco de inicio personalizado) para arrancar el sistema de destino
- Direcciones IP estáticas válidas ya asignadas a la fuente de la instalación y al sistema de control
- Dirección IP estática válida para asignar al sistema de destino

Para realizar este tipo de instalación, siga estos pasos:

1. Configure la fuente de la instalación tal y como se describe en la Sección 1.2, "Configuración del servidor que almacena las fuentes de la instalación" (p. 27).
2. Arranque el sistema de destino mediante el primer CD o DVD del kit de medios de SUSE Linux.
3. Cuando aparezca la pantalla de arranque del sistema de destino, utilice el menú de opciones de arranque para establecer los parámetros apropiados de la conexión de red, la dirección de la fuente de la instalación y la habilitación de SSH. Esto se describe con más detalle en la Sección 1.4.3, "Uso de opciones de arranque personalizadas" (p. 49).

   El sistema de destino inicia un entorno basado en texto y ofrece la dirección de red que los clientes SSH pueden utilizar para acceder al entorno de instalación gráfica.
4. En la estación de trabajo de control, abra una ventana de terminal y conéctese al sistema de destino como se describe en "Conexión al programa de instalación" (p. 54).
5. Realice la instalación como se describe en el Capítulo *Instalación mediante YaST* (↑Inicio).

Es necesario volver a conectarse al sistema de destino después de reiniciarlo para la parte final de la instalación.

6 Complete la instalación.

1.1.5 Instalación remota sencilla mediante SSH: configuración de red dinámica mediante DHCP

Para este tipo de instalación es necesario un cierto grado de acceso físico al sistema de destino con el fin de arrancarlo para la instalación y de determinar la dirección IP del destino de la instalación. Una estación de trabajo remota controla completamente la instalación propiamente dicha y usa VNC para conectarse al programa de instalación, pero es necesaria la intervención del usuario para realizar la configuración.

Para este tipo de instalación, asegúrese de que se cumplen los siguientes requisitos:

- Fuente de la instalación remota: NFS, HTTP, FTP o SMB con una conexión de red en funcionamiento
- Sistema de destino con una conexión de red en funcionamiento
- Sistema de control con una conexión de red y software cliente para SSH en funcionamiento
- Medio de arranque físico (CD o DVD) para arrancar el sistema de destino
- Servidor DHCP en funcionamiento que suministre las direcciones IP

Para realizar este tipo de instalación, siga estos pasos:

1 Configure la fuente de la instalación tal y como se describe en la Sección 1.2, “Configuración del servidor que almacena las fuentes de la instalación” (p. 27). Escoja un servidor de red NFS, HTTP o FTP. Si la fuente de la instalación es SMB, consulte la Sección 1.2.5, “Gestión de una fuente de instalación SMB” (p. 35).

2 Arranque el sistema de destino mediante el primer CD o DVD del kit de medios de SUSE Linux.

3 Cuando aparezca la pantalla de arranque en el sistema de destino, utilice el menú de opciones de arranque para establecer los parámetros apropiados de la conexión de red, la dirección de la fuente de la instalación y la habilitación de SSH. Para obtener instrucciones detalladas sobre el uso de estos parámetros, consulte la Sección 1.4.3, “Uso de opciones de arranque personalizadas” (p. 49).

   El sistema de destino inicia un entorno basado en texto y ofrece la dirección de red mediante la cual los clientes SSH pueden dirigirse al entorno de instalación gráfica.

4 En la estación de trabajo de control, abra una ventana de terminal y conéctese al sistema de destino como se describe en “Conexión al programa de instalación” (p. 54).

5 Realice la instalación como se describe en el Capítulo *Instalación mediante YaST* (↑Inicio).

   Es necesario volver a conectarse al sistema de destino después de reiniciarlo para la parte final de la instalación.

6 Complete la instalación.

1.1.6 Instalación remota mediante SSH: arranque en PXE y Wake on LAN

Este tipo de instalación no requiere intervención física alguna. La máquina de destino se inicia y arranca de manera remota.

Para este tipo de instalación, asegúrese de que se cumplen los siguientes requisitos:

- Fuente de la instalación remota: NFS, HTTP, FTP o SMB con una conexión de red en funcionamiento
- Servidor TFTP
- Servidor DHCP en funcionamiento en la red que proporcione una dirección IP estática para el host que se vaya a instalar

- Sistema de destino compatible con arranque en PXE, funcionamiento en red y Wake on LAN, enchufado y conectado a la red
- Sistema de control con una conexión de red en funcionamiento y software cliente para SSH

Para realizar este tipo de instalación, siga los pasos siguientes:

1. Configure la fuente de la instalación tal y como se describe en la Sección 1.2, “Configuración del servidor que almacena las fuentes de la instalación” (p. 27). Escoja un servidor de red NFS, HTTP o FTP. Para configurar una fuente de instalación SMB, consulte la Sección 1.2.5, “Gestión de una fuente de instalación SMB” (p. 35).

2. Configure un servidor TFTP para que almacene una imagen de arranque que pueda ser utilizada por el sistema de destino. Esto se describe en la Sección 1.3.2, “Configuración de un servidor TFTP” (p. 38).

3. Configure un servidor DHCP para que suministre direcciones IP a todas las máquinas e indique la ubicación del servidor TFTP al sistema de destino. Esto se describe en la Sección 1.3.1, “Configuración de un servidor DHCP” (p. 37).

4. Prepare el sistema de destino para arranque en PXE. Esto se describe con más detalle en la Sección 1.3.5, “Preparación del sistema de destino para arranque en PXE” (p. 45).

5. Comience el proceso de arranque del sistema de destino mediante Wake on LAN. Esto se describe en la Sección 1.3.7, “Wake on LAN” (p. 46).

6. En la estación de trabajo de control, abra un cliente SSH y conéctese al sistema de destino como se describe en la Sección 1.5.2, “Instalación con SSH” (p. 54).

7. Realice la instalación como se describe en el Capítulo *Instalación mediante YaST* (↑Inicio).

   Es necesario volver a conectarse al sistema de destino después de reiniciarlo para la parte final de la instalación.

8. Complete la instalación.

1.2 Configuración del servidor que almacena las fuentes de la instalación

En función del sistema operativo instalado en la máquina que se utilizará como fuente de la instalación en red para SUSE Linux, existen varias opciones para configurar el servidor. En SUSE LINUX Enterprise Server o SUSE Linux 9.3 o posterior, la manera más sencilla de configurar un servidor de instalación es utilizar YaST. En otras versiones de SUSE LINUX Enterprise Server o SUSE Linux, configure la fuente de la instalación de manera manual.

SUGERENCIA

Es posible incluso utilizar una máquina con Microsoft Windows como servidor de la instalación para la instalación de Linux. Para obtener más información, consulte la Sección 1.2.5, “Gestión de una fuente de instalación SMB” (p. 35).

1.2.1 Configuración de un servidor de instalación mediante YaST

YaST ofrece una herramienta gráfica para la creación de fuentes de instalación en red. Admite servidores de instalación en red HTTP, FTP y NFS.

1. Inicie sesión como usuario root en la máquina que actuará como servidor de la instalación.
2. Inicie *YaST → Otros → Servidor de instalación*.
3. Seleccione *Configuración del servidor*.
4. Seleccione el tipo de servidor (HTTP, FTP o NFS).

   El servicio del servidor seleccionado se ejecuta automáticamente cada vez que se inicia el sistema. Si ya se encuentra en funcionamiento en el sistema un servicio del tipo seleccionado y desea configurarlo manualmente para el servidor, desactive

la configuración automática del servicio del servidor mediante *No configurar ningún servicio de red.* En ambos casos, defina el directorio en el que los datos de la instalación estarán disponibles en el servidor.

5 Configure el tipo de servidor requerido.

Este paso está relacionado con la configuración automática de servicios de servidor. Se omite cuando la configuración automática está desactivada. Defina un alias para el directorio raíz del servidor FTP o HTTP en el que se encontrarán los datos de la instalación. La fuente de la instalación se ubicará más adelante en `ftp://IP_del_servidor/alias/nombre` (FTP) o en `http://IP_del_servidor/alias/nombre` (HTTP). *`nombre`* representa el nombre de la fuente de la instalación, que se define en el siguiente paso. Si ha seleccionado NFS en el paso anterior, defina los comodines y las opciones de exportación. Podrá acceder al servidor NFS en `nfs://IP_del_servidor/nombre`. Se pueden encontrar más detalles sobre NFS y las exportaciones en el Capítulo 22, *Uso compartido de sistemas de archivos con NFS* (p. 431).

6 Configure la fuente de la instalación.

Antes de que los medios de instalación se copien en el destino, defina el nombre de la fuente de la instalación (lo ideal sería una abreviación fácil de recordar del producto y la versión). YaST permite ofrecer imágenes ISO de los medios en lugar de copias de los CDs de instalación. Si desea hacerlo así, active la casilla de verificación correspondiente y especifique la vía del directorio en el que se ubican localmente los archivos ISO. En función del producto que se distribuya mediante este servidor de instalación, es posible que se necesiten CD complementarios o de paquetes de servicio para instalarlo completamente. Si activa *Pedir CD adicionales*, YaST le recordará automáticamente que añada estos medios. Para anunciar en la red el servidor de instalación mediante OpenSLP, active la opción correspondiente.

SUGERENCIA

Considere la opción de anunciar la fuente de la instalación mediante OpenSLP si la red lo admite. Esto le evita el tener que introducir la vía de instalación en red en cada máquina de destino. Los sistemas de destino se arrancarán con la opción de arranque en SLP y encontrarán la fuente de la instalación en red sin necesidad de configuración adicional. Para

obtener más detalles sobre esta opción, consulte la Sección 1.4, “Arranque del sistema de destino para la instalación” (p. 47).

7 Cargue los datos de la instalación.

El paso que más tiempo ocupa durante la configuración de un servidor de instalación es el copiado de los CDs de instalación en sí. Introduzca los medios en el orden que YaST solicite y espere a que termine el proceso de copiado. Cuando las fuentes se hayan copiado completamente, vuelva al resumen de las fuentes de información existentes y cierre la configuración seleccionando *Finalizar*.

El servidor de instalación quedará completamente configurado y listo para usarse. Se ejecutará automáticamente cada vez que se inicie el sistema. No es necesario intervenir de ninguna otra manera. Sólo es necesario configurar e iniciar correctamente este servicio a mano si se desactiva la configuración automática del servicio de red seleccionado con YaST en el paso inicial.

Para desactivar una fuente de instalación, seleccione *Cambiar* en el resumen para obtener una lista de todas las fuentes de instalación disponibles. Elija la entrada que desee borrar y seleccione *Suprimir*. Este procedimiento de eliminación sólo implica la desactivación del servicio del servidor. Los datos de la instalación en sí permanecen en el directorio escogido. No obstante, es posible eliminarlos de forma manual.

Si el servidor de instalación ofrece datos de instalación para más de un producto o versión, inicie el módulo del servidor de instalación de YaST y seleccione *Configurar* en el resumen de las fuentes de instalación existentes para configurar la nueva fuente de instalación.

1.2.2 Configuración manual de una fuente de instalación NFS

La configuración de una fuente de instalación NFS se lleva a cabo básicamente en dos pasos. En primer lugar, cree la estructura de directorios en la que se almacenarán los datos de la instalación y copie los medios de instalación en dicha estructura. A continuación, exporte a la red el directorio que contiene los datos de la instalación.

Para crear un directorio en el que se almacenen los datos de la instalación, siga los pasos siguientes:

1 Inicie sesión como usuario Root.

2 Cree un directorio en el que más adelante se almacenarán los datos de la instalación y cambie a dicho directorio. Por ejemplo:

```
mkdir install/producto/versiondelproducto
cd install/producto/versiondelproducto
```

Sustituya *producto* por una abreviación del nombre del producto (en este caso, SUSE Linux) y *versiondelproducto* por una cadena que contenga el nombre del producto y la versión.

3 Ejecute los siguientes comandos para cada CD contenido en el kit de medios:

a Copie el contenido completo del CD de instalación en el directorio del servidor de instalación:

```
cp -a /media/via_a_la_unidad_de_CD-ROM .
```

Sustituya *via_a_la_unidad_de_CD-ROM* por la vía real por la que se accede a la unidad de CD o DVD. En función del tipo de unidad utilizado en el sistema, la vía puede ser `cdrom`, `cdrecorder`, `dvd` o `dvdrecorder`.

b Cambie el nombre del directorio al número del CD:

```
mv via_a_la_unidad_de_CD-ROM CDx
```

Sustituya *x* por el número real del CD.

Para exportar las fuentes de la instalación mediante NFS con YaST, siga estos pasos:

1 Inicie sesión como usuario Root.

2 Inicie *YaST → Servicios de red → Servidor NFS*.

3 Seleccione *Iniciar el servidor NFS* y *Puerto abierto en el cortafuegos*, y haga clic en *Siguiente*.

4 Seleccione *Añadir directorio* e introduzca la vía del directorio que contiene los datos de la instalación. En este caso, corresponde a `/versiondelproducto`.

5 Seleccione *Añadir equipo* e introduzca los nombres de host de las máquinas a las que se exportarán los datos de la instalación. En lugar de especificar aquí los nombres de host, es posible usar comodines, rangos de direcciones de red o simplemente el nombre de dominio de la red. Introduzca las opciones de exportación apropiadas o mantenga las que se ofrecen por defecto, las cuales funcionan correctamente en la mayoría de las configuraciones. Para obtener más información sobre la sintaxis utilizada en la exportación de recursos compartidos NFS, lea la página Man de `exports`.

6 Haga clic en *Finalizar*.

El servidor NFS en el que se almacenan las fuentes de la instalación de SUSE Linux se iniciará automáticamente y se integrará en el proceso de arranque.

Si prefiere exportar las fuentes de la instalación mediante NFS de manera manual en lugar de utilizar el módulo Servidor NFS de YaST, siga estos pasos:

1 Inicie sesión como usuario Root.

2 Abra el archivo `/etc/exports` e introduzca la siguiente línea:

```
/versiondelproducto *(ro,root_squash,sync)
```

Con ello se exporta el directorio `/versiondelproducto` a cualquier host que forme parte de la red o a cualquier host que se conecte al servidor. Para limitar el acceso al servidor, utilice máscaras de red o nombres de dominio en lugar del comodín general `*`. Consulte la página Man de `export` para obtener más detalles. Guarde y salga del archivo de configuración.

3 Para añadir el servicio NFS a la lista de servidores que se inicia durante el arranque del sistema, ejecute los siguientes comandos:

```
insserv /etc/init.d/nfsserver
insserv /etc/init.d/portmap
```

4 Inicie el servidor NFS con el siguiente comando:

```
rcnfsserver start
```

Si más adelante necesita cambiar la configuración del servidor NFS, modifique el archivo de configuración y reinicie el daemon NFS con `rcnfsserver restart`.

El anuncio del servidor NFS mediante OpenSLP hace que todos los clientes de la red conozcan su dirección.

1. Inicie sesión como usuario Root.
2. Entre en el directorio `/etc/slp.reg.d/`.
3. Cree un archivo de configuración con el nombre `install.suse.nfs.reg` que contenga las siguientes líneas:

   ```
   # Register the NFS Installation Server
   service:install.suse:nfs://$HOSTNAME/path_instsource/CD1,en,65535
   description=NFS Installation Source
   ```

   Sustituya *`via_fuenteinst`* por la vía real a la fuente de la instalación en el servidor.
4. Guarde este archivo de configuración e inicie el daemon OpenSLP con el siguiente comando:

   ```
   rcslpd start
   ```

Para obtener más información sobre OpenSLP, consulte el paquete de documentación que se encuentra en `/usr/share/doc/packages/openslp/` y también el Capítulo 19, *Servicios SLP en la red* (p. 393).

1.2.3 Configuración manual de una fuente de instalación FTP

La creación de una fuente de instalación FTP es muy similar a la creación de una fuente de instalación NFS. Las fuentes de instalación FTP también se pueden anunciar en la red mediante OpenSLP.

1. Cree un directorio en el que se almacenarán las fuentes de la instalación como se describe en la Sección 1.2.2, “Configuración manual de una fuente de instalación NFS” (p. 29).
2. Configure el servidor FTP para que distribuya los contenidos del directorio de instalación:

a Inicie sesión como usuario root e instale el paquete `pure-ftpd` (un pequeño servidor FTP) con el gestor de paquetes de YaST.

b Entre en el directorio raíz del servidor FTP:

```
cd/srv/ftp
```

c Cree un subdirectorio en el que se almacenarán las fuentes de la instalación en el directorio raíz FTP:

```
mkdir fuenteinst
```

Sustituya *`fuenteinst`* por el nombre del producto.

d Copie el contenido de todos los CDs de instalación en el directorio raíz del servidor FTP (de manera similar al procedimiento descrito en la Sección 1.2.2, “Configuración manual de una fuente de instalación NFS” (p. 29), Paso 3 (p. 30)).

También puede montar los contenidos del repositorio de instalación existente en el entorno chroot del servidor FTP:

```
mount --bind via_a_fuenteinst /srv/ftp/fuenteinst
```

Sustituya *`via_a_fuenteinst`* y *`fuenteinst`* con los valores correspondientes a su configuración. Si necesita que sea permanente, añádalo a `/etc/fstab`.

e Inicie pure-ftpd:

```
pure-ftpd &
```

3 Anuncie la fuente de la instalación mediante OpenSLP si la configuración de la red lo admite:

a Cree un archivo de configuración con el nombre `install.suse.ftp.reg` en `/etc/slp/reg.d/` que contenga las siguientes líneas:

```
# Register the FTP Installation Server
service:install.suse:ftp://$HOSTNAME/srv/ftp/instsource/CD1,en,65535
description=FTP Installation Source
```

Sustituya *`fuenteinst`* por el nombre real de la fuente de la instalación en el servidor. La línea `service:` debe introducirse en una sola línea.

b Guarde este archivo de configuración e inicie el daemon OpenSLP con el siguiente comando:

```
rcslpd start
```

1.2.4 Configuración manual de una fuente de instalación HTTP

La creación de una fuente de instalación HTTP es muy similar a la creación de una fuente de instalación NFS. Las fuentes de instalación HTTP también se pueden anunciar en la red mediante OpenSLP.

1. Cree un directorio en el que se almacenarán las fuentes de la instalación como se describe en la Sección 1.2.2, “Configuración manual de una fuente de instalación NFS” (p. 29).

2. Configure el servidor HTTP para que distribuya los contenidos del directorio de instalación:

   a Instale el servidor Web Apache como se describe en la Sección 26.1.2, “Instalación” (p. 484).

   b Entre en el directorio raíz del servidor HTTP (`/srv/www/htdocs`) y cree un subdirectorio en el que se almacenarán las fuentes de la instalación:

   ```
   mkdir instsource
   ```

   Sustituya *`fuenteinst`* por el nombre del producto.

   c Cree un enlace simbólico entre la ubicación de las fuentes de la instalación y el directorio raíz del servidor Web (`/srv/www/htdocs`):

   ```
   ln -s /via_fuenteinst /srv/www/htdocs/fuenteinst
   ```

   d Modifique el archivo de configuración del servidor HTTP (`/etc/apache2/default-server.conf`) para que siga enlaces simbólicos. Sustituya la siguiente línea:

   ```
   Options None
   ```

con

```
Options Indexes FollowSymLinks
```

e Vuelva a cargar la configuración del servidor HTTP con `rcapache2 restart`.

3 Anuncie la fuente de la instalación mediante OpenSLP si la configuración de la red lo admite:

a Cree un archivo de configuración con el nombre `install.suse.http.reg` en `/etc/slp/reg.d/` que contenga las siguientes líneas:

```
# Register the HTTP Installation Server
service:install.suse:http://$HOSTNAME/srv/www/htdocs/instsource/CD1/,en,65535
description=HTTP Installation Source
```

Sustituya *`via_a_fuenteinst`* por la vía real en la fuente de la instalación en el servidor. La línea `service:` debe introducirse en una sola línea.

b Guarde este archivo de configuración e inicie el daemon OpenSLP con el comando `rcslpd restart`.

1.2.5 Gestión de una fuente de instalación SMB

Mediante SMB (Samba) es posible importar las fuentes de la instalación de un servidor Microsoft Windows e iniciar la instalación de Linux incluso sin que haya ninguna máquina Linux.

Para configurar un recurso compartido de Windows en el que se almacenarán las fuentes de la instalación de SUSE Linux, siga estos pasos:

1 Inicie sesión en la máquina que tenga instalado Windows.

2 Inicie el explorador y cree una nueva carpeta en la que se almacenará el árbol de la instalación completo y déle como nombre, por ejemplo, `INSTALL`.

3 Exporte este recurso compartido mediante el procedimiento descrito en la documentación de Windows.

4 Entre en dicho recurso compartido y cree una subcarpeta de nombre *producto*. *producto* debe reemplazarse por el nombre real del producto (en este caso, SUSE Linux).

5 Copie cada CD de SUSE Linux en una carpeta diferente y llame a estas carpetas `CD1`, `CD2`, `CD3` etc.

6 Entre en el directorio superior del recurso compartido exportado (en este ejemplo, `INSTALL`) y copie a esta carpeta los siguientes archivos y carpetas de *producto*`/CD1`: `content`, `media.1`, `control.xml` y `boot`.

7 Cree una nueva carpeta bajo `INSTALL` de nombre `yast`.

Entre en la carpeta `yast` y cree los archivos `order` e `instorder`.

8 Abra el archivo `order` e introduzca la siguiente línea:

```
/NLD/CD1 smb://usuario:contraseña@nombredelhost/productoCD1
```

Sustituya *usuario* por el nombre de usuario que utilice en la máquina Windows o utilice `Guest` para permitir un inicio de sesión como invitado a este recurso compartido. *contraseña* debe sustituirse o bien por la contraseña de inicio de sesión o bien por una cadena cualquiera en el caso de inicio de sesión como invitado. *nombredelhost* debe sustituirse por el el nombre de red de la máquina Windows.

9 Abra el archivo `instorder` y añada la siguiente línea:

```
/producto/CD1
```

Para utilizar un recurso compartido SMB montado como fuente de la instalación, siga los pasos siguientes:

1 Arranque el destino de la instalación.

2 Seleccione *Instalación*.

3 Pulse F3 y F4 para ver una selección de fuentes de instalación.

4 Seleccione SMB e introduzca el nombre o la dirección IP de la máquina Windows, el nombre del recurso compartido (en este ejemplo, `INSTALL`), el nombre de usuario y la contraseña.

Cuando pulse Intro, YaST se iniciará y podrá realizar la instalación.

1.3 Preparación del arranque del sistema de destino

En esta sección se describen las tareas de configuración necesarias en entornos de arranque complejos. Contiene ejemplos de configuración listos para usar para DHCP, arranque en PXE, TFTP y Wake on LAN.

1.3.1 Configuración de un servidor DHCP

La configuración de servidores DHCP en SUSE Linux se realiza mediante la edición manual de los archivos de configuración correspondientes. En esta sección se describe la ampliación de la configuración de un servidor DHCP existente para que ofrezca los datos necesarios para servir en un entorno TFTP, PXE y WOL.

Configuración manual de un servidor DHCP

Todo lo que necesita hacer el servidor DHCP, además de ofrecer asignación de direcciones automática a los clientes de la red, es anunciar la dirección IP del servidor TFTP y el archivo que las rutinas de instalación de la máquina de destino deben obtener.

1 Inicie sesión como usuario root en la máquina que aloje el servidor DHCP.

2 Añada las siguientes líneas al archivo de configuración del servidor DHCP que se encuentra en `/etc/dhcpd.conf`:

```
group {
  # PXE related stuff
  #
  # "next server" defines the tftp server that will be used
  next server ip_del_servidor_tftp:
  #
  # "filename" specifiies the pxelinux image on the tftp server
```

```
  # the server runs in chroot under /srv/tftpboot
  filename  "pxelinux.0";
}
```

Sustituya *ip_del_servidor_tftp* con la dirección IP real del servidor TFTP.

Para obtener más información acerca las opciones disponibles en `dhcpd.conf`, consulte la página de Man de `dhcpd.conf`.

3. Reinicie el servidor DHCP ejecutando `rcdhcpd restart`.

Si tiene previsto utilizar SSH para controlar remotamente una instalación PXE y Wake on LAN, especifique explícitamente la dirección IP que DHCP debe suministrar al destino de la instalación. Para ello, modifique la configuración DHCP antes mencionada de acuerdo con el siguiente ejemplo:

```
group {
  # PXE related stuff
  #
  # "next server" defines the tftp server that will be used
  next server ip_del_servidor_tftp:
  #
  # "filename" specifiies the pxelinux image on the tftp server
  # the server runs in chroot under /srv/tftpboot
  filename "pxelinux.0";
  host test { hardware ethernet direccion_mac;
              fixed-address alguna_direccion_ip; }
      }
```

La declaración del host incluye el nombre del host del destino de la instalación. Para relacionar el nombre de host y la dirección IP con un host determinado, es necesario conocer y especificar la dirección de hardware del sistema (MAC). Sustituya todas las variables utilizadas en este ejemplo por los valores reales correspondientes a su entorno.

Una vez reiniciado el servidor DHCP, ofrecerá una dirección IP estática al host especificado, lo que permitirá conectarse al sistema mediante SSH.

1.3.2 Configuración de un servidor TFTP

La configuración de servidores TFTP se puede realizar con YaST, o bien de forma manual en cualquier otro sistema operativo Linux que sea compatible con xinetd y tftp. El servidor TFTP proporciona la imagen de arranque al sistema de destino cuando éste arranca y envía una solicitud para ello.

Configuración de un servidor TFTP mediante YaST

1. Inicie sesión como usuario Root.
2. Inicie *YaST → Servicios de red → Servidor TFTP* e instale el paquete necesario.
3. Haga clic en *Habilitar* para asegurarse de que el servidor se inicie y se incluya en las rutinas de arranque. No es necesaria ninguna otra intervención por su parte para ello. xinetd inicia tftpd en el momento del arranque.
4. Haga clic en *Puerto abierto en el cortafuegos* para abrir el puerto correspondiente en el cortafuegos que se esté ejecutando en la máquina. Si no hay ningún cortafuegos en ejecución en el servidor, está opción no estará disponible.
5. Haga clic en *Examinar* para explorar el directorio de la imagen de arranque.

   Se creará y se seleccionará automáticamente el directorio por defecto `/tftpboot`.
6. Haga clic en *Finalizar* para aplicar la configuración e iniciar el servidor.

Configuración manual de un servidor TFTP

1. Inicie sesión como usuario root e instale los paquetes `tftp` y `xinetd`.
2. Si no están disponibles, cree los directorios `/srv/tftpboot` y `/srv/tftpboot/pxelinux.cfg`.
3. Añada los archivos correspondientes necesarios para la imagen de arranque como se describe en la Sección 1.3.3, “Arranque en PXE” (p. 40).
4. Modifique la configuración de xinetd, que se encuentra en `/etc/xinetd.d/` para asegurarse de que el servidor tftp se inicie durante el arranque:

   a. Si no existe, cree un archivo de nombre `tftp` en este directorio mediante `touch tftp`. A continuación, ejecute `chmod 755 tftp`.

   b. Abra el archivo `tftp` y añada las siguientes líneas:

   ```
   service tftp
   {
   ```

```
        socket_type             = dgram
        protocol                = udp
        wait                    = yes
        user                    = root
        server                  = /usr/sbin/in.tftpd
        server_args             = -s /tftpboot
        disable                 = no
}
```

c Guarde el archivo y reinicie xinetd con `rcxinetd restart`.

1.3.3 Arranque en PXE

En las especificaciones de Preboot Execution Environment (PXE), disponibles en `ftp://download.intel.com/labs/manage/wfm/download/pxespec.pdf`, se incluye información técnica básica, así como las especificaciones completas de PXE.

1 Cambie al directorio del repositorio de la instalación y copie los archivos `linux`, `initrd`, `message` y `memtest` en el directorio `/srv/tftpboot` introduciendo lo siguiente:

```
cp -a boot/loader/linux boot/loader/initrd
      boot/loader/message boot/loader/memtest /srv/tftpboot
```

2 Instale el paquete `syslinux` directamente desde los CDs o DVDs de instalación con YaST.

3 Copie el archivo `/usr/share/syslinux/pxelinux.0` en el directorio `/srv/tftpboot` introduciendo lo siguiente:

```
cp -a /usr/share/syslinux/pxelinux.0 /srv/tftpboot
```

4 Cambie al directorio del repositorio de la instalación y copie el archivo `isolinux.cfg` en el directorio `/srv/tftpboot/pxelinux.cfg/default` introduciendo lo siguiente:

```
cp -a boot/loader/isolinux.cfg /srv/tftpboot/pxelinux.cfg/default
```

5 Edite el archivo `/srv/tftpboot/pxelinux.cfg/default` y elimine las líneas que comiencen por `gfxboot`, `readinfo` y `framebuffer`.

6 Añada las siguientes entradas en las líneas append de las etiquetas por defecto `failsafe` y `apic`:

`insmod=e100`
: Mediante esta entrada, se carga en los clientes PXE el módulo del núcleo para tarjetas de red de 100 MBits/s de Intel. Esta entrada depende del hardware del cliente y debe adaptarse en consecuencia. En caso de utilizar una tarjeta de red GigaBit de Broadcom, la entrada debería ser `insmod=bcm5700`.

`netdevice=eth0`
: Esta entrada define la interfaz de red del cliente que debe utilizarse para la instalación en red. Sólo es necesaria si el cliente dispone de varias tarjetas de red y debe adaptarse en consecuencia. En el caso de que sólo se disponga de una tarjeta de red, esta entrada debe omitirse.

`install=nfs://`*`ip_servidorinst/via_fuenteinst`*`/CD1`
: Esta entrada define el servidor NFS y la fuente de la instalación para la instalación del cliente. Sustituya *`ip_servidorinst`* por la dirección IP real del servidor de la instalación. *`via_fuenteinst`* debe sustituirse por la vía real a las fuentes de la instalación. Las direcciones de las fuentes HTTP, FTP y SMB son similares, excepto en el prefijo del protocolo, que debe ser `http`, `ftp` o `smb`.

IMPORTANTE

Si necesita pasar otras opciones de arranque a las rutinas de instalación, tales como parámetros de inicio de VNC o SSH, añádalas a la entrada `install`. En la Sección 1.4, “Arranque del sistema de destino para la instalación” (p. 47) se ofrece un resumen de los parámetros y algunos ejemplos.

A continuación se incluye un ejemplo de archivo `/srv/tftpboot/pxelinux.cfg/default`. Ajuste el prefijo del protocolo de la fuente de la instalación para que se corresponda con la configuración de la red, y especifique el método que prefiera para conectarse al instalador añadiendo las opciones `vnc` y `vncpassword` o `ssh` y `sshpassword` a la entrada `install`. Las líneas separadas por \ deben introducirse en una sola línea, sin salto de línea y sin \.

```
default linux

# default
label linux
  kernel linux
        append initrd=initrd ramdisk_size=65536 insmod=e100 \
        install=nfs://ip_instserver/path_instsource/product

# failsafe
label failsafe
  kernel linux
  append initrd=initrd ramdisk_size=65536 ide=nodma apm=off acpi=off \

  insmod=e100 install=nfs://ip_servidorinst/via_fuenteinst/producto

# apic
label apic
  kernel linux
  append initrd=initrd ramdisk_size=65536 apic insmod=e100 \
  install=nfs://ip_servidorinst/via_fuenteinst/producto

# manual
label manual
  kernel linux
  append initrd=initrd ramdisk_size=65536 manual=1

# rescue
label rescue
  kernel linux append initrd=initrd ramdisk_size=65536 rescue=1

#  memory test
label memtest
  kernel memtest

# hard disk
label harddisk
  kernel
  linux append SLX=0x202

implicit     0
display      message
prompt       1
timeout      100
```

Sustituya *ip_servidorinst* y *via_fuenteinst* por los valores correspondientes a su configuración.

La siguiente sección sirve como breve referencia de las opciones de PXELINUX utilizadas en esta configuración. Hay más información sobre las opciones disponibles en la documentación del paquete `syslinux` que se encuentra en `/usr/share/doc/packages/syslinux/`.

1.3.4 Opciones de configuración de PXELINUX

A continuación aparecen algunas de las opciones disponibles para el archivo de configuración de PXELINUX.

`DEFAULT` *`opciones del núcleo...`*
: Establece la línea de comandos del núcleo por defecto. Si PXELINUX arranca de manera automática, actúa como si las entradas posteriores a DEFAULT se hubieran escrito en el indicador de inicio, excepto la opción auto que se añade de manera automática, lo que indica un arranque automático.

  Si no hay ningún archivo de configuración o ninguna entrada DEFAULT en el archivo de configuración, el valor por defecto es el nombre del núcleo "linux", sin opciones.

`APPEND` *`opciones...`*
: Añada una o más opciones a la línea de comandos del núcleo. Éstas se añaden para arranques automáticos y manuales. Las opciones se añaden al principio de la línea de comandos del núcleo, y normalmente admiten que las opciones del núcleo introducidas explícitamente las sobrescriban.

`LABEL` *`etiqueta`* `KERNEL` *`imagen`* `APPEND` *`opciones...`*
: Indica que si se introduce *`etiqueta`* como el núcleo que se debe arrancar, PXELINUX debe arrancar *`imagen`* en su lugar y utilizar las opciones APPEND especificadas en lugar de las indicadas en el apartado global del archivo (antes del primer comando LABEL). El valor por defecto de *`imagen`* es el mismo que *`label`* y, si no se introduce ningún APPEND, el valor por defecto consiste en utilizar la entrada global (si hubiera alguna). Se permiten hasta 128 entradas LABEL.

  Tenga en cuenta que GRUB utiliza la siguiente sintaxis:

```
title mytitle
  kernel mi_nucleo mis_opciones_del_nucleo
  initrd miinitrd
```

  mientras que PXELINUX utiliza la siguiente:

```
label mietiqueta
  kernel minucleo
  append misopciones
```

Las etiquetas se truncan como si fueran nombres de archivo, y deben ser únicas después del truncamiento. Por ejemplo, dos etiquetas como “v2.1.30” y “v2.1.31” no podrán distinguirse en PXELINUX porque ambas se truncan con el mismo nombre de archivo de DOS.

No es necesario que el núcleo sea un núcleo de Linux; puede ser un sector de arranque o un archivo COMBOOT.

APPEND -
: Sin nada añadido. Se puede utilizar `APPEND` con un solo guión como argumento en un apartado `LABEL` para sobrescribir un `APPEND` global.

`LOCALBOOT` *`tipo`*
: En PXELINUX, especificar `LOCALBOOT 0` en lugar de una opción de `KERNEL` significa la invocación de esa etiqueta en particular y provoca un arranque del disco local en lugar de un arranque del núcleo.

Argumento	Descripción
`0`	Realiza un arranque normal
`4`	Realiza un arranque local con el controlador Universal Network Driver Interface (UNDI) aún residente en memoria
`5`	Realiza un arranque local con el stack de PXE completo, incluido el controlador UNDI, aún residente en memoria

Los demás valores no están definidos. Si desconoce los stacks UNDI o PXE, especifique `0`.

`TIMEOUT` *`tiempo límite`*
: Indica cuánto tiempo deberá esperar en el indicador de inicio antes de arrancar automáticamente, en décimas de segundo. El tiempo límite queda cancelado si el usuario pulsa alguna tecla, en cuyo caso se asume que será éste quien complete el comando iniciado. Un tiempo límite de cero inhabilita la opción de tiempo límite (es el ajuste por defecto).

El máximo valor posible para el valor del tiempo límite es de 35996 (algo menos de una hora).

PROMPT *valor_de_indicador*

Si `valor de indicador` es 0, muestra el indicador de inicio sólo si se pulsan las teclas Shift o Alt o si están activados Bloq Mayús o Bloq Despl (es la opción por defecto). Si `valor_de_indicador` es 1, siempre se muestra el indicador de inicio.

```
F1  nombre_de_archivo
F2  nombre_de_archivo
...
F9  nombre_de_archivo
F10nombre_de_archivo
```

Muestra en la pantalla el archivo indicado cuando se pulsa una tecla de función en el indicador de inicio. También se puede utilizar para implementar una ayuda en línea para antes del arranque (normalmente para las opciones de la línea de comandos del núcleo). Por compatibilidad con versiones anteriores, F10 también puede introducirse como F0. Tenga en cuenta que no es posible asociar nombres de archivos a F11 ni F12.

1.3.5 Preparación del sistema de destino para arranque en PXE

Prepare el BIOS del sistema para arranque en PXE incluyendo la opción de PXE en el orden de arranque del BIOS.

AVISO

No coloque la opción de PXE por encima de la opción de arranque desde disco duro en el BIOS. De lo contrario, el sistema intentaría reinstalarse cada vez que lo arrancara.

1.3.6 Preparación del sistema de destino para Wake on LAN

Wake on LAN (WOL) necesita que se habilite la opción correspondiente del BIOS antes de la instalación. Además, es necesario tomar nota de la dirección MAC del sistema de destino. Este dato es necesario para iniciar Wake on LAN.

1.3.7 Wake on LAN

Wake on LAN permite conectar una máquina mediante el envío de un paquete de red especial que contiene la dirección MAC de la máquina. Dado que los identificadores MAC deben ser únicos para cada máquina, no hay que preocuparse por la conexión accidental de la máquina que no es.

IMPORTANTE

Si la máquina de control no se encuentra en el mismo segmento de red que el destino de la instalación que debe encenderse, configure las peticiones WOL para que se envíen como multidifusión o bien controle remotamente una máquina de dicho segmento de red para que actúe como remitente de las peticiones.

1.3.8 Wake on LAN manual

1. Inicie sesión como usuario Root.
2. Inicie *YaST → Instalar/desinstalar software* e instale el paquete `netdiag`.
3. Abra un terminal e introduzca el siguiente comando como usuario root para encender el destino.

   ```
   ether-wake mac_del_destino
   ```

   Sustituya *`mac_del_destino`* por la dirección MAC real del destino.

1.4 Arranque del sistema de destino para la instalación

Existen básicamente dos maneras diferentes de personalizar el proceso de arranque para la instalación además de las mencionadas en la Sección 1.3.7, “Wake on LAN” (p. 46) y en la Sección 1.3.3, “Arranque en PXE” (p. 40). Es posible utilizar las opciones de arranque por defecto y las teclas de función o bien utilizar las opciones del menú de opciones de arranque de la pantalla de arranque de la instalación para pasar las opciones de arranque que el núcleo de la instalación pueda necesitar para este hardware en concreto.

1.4.1 Uso de las opciones de arranque por defecto

Las opciones de arranque se describen con detalles en el Capítulo *Instalación mediante YaST* (↑Inicio).

En general, el proceso de arranque de la instalación se inicia con sólo seleccionar *Instalación*. Si se detectan problemas, utilice *Instalación - ACPI desactivado* o *Instalación - Ajustes seguros.*

Para obtener más información acerca de solución de problemas durante el proceso de instalación, consulte la Sección “Problemas de instalación” (Capítulo 9, *Problemas comunes y sus soluciones*, ↑Inicio).

1.4.2 Uso de las teclas de función

La barra de menú de la parte inferior de la pantalla ofrece algunas funciones avanzadas que son necesarias en determinadas configuraciones. Mediante las teclas de función es posible especificar opciones adicionales que se pasarán a las rutinas de instalación sin tener que conocer la sintaxis detallada de dichos parámetros que sería necesaria para introducirlos como opciones de arranque (consulte la Sección 1.4.3, “Uso de opciones de arranque personalizadas” (p. 49)).

Consulte la siguiente tabla para ver las opciones disponibles.

Tabla 1.1 *Teclas de función durante la instalación*

Tecla	Finalidad	Opciones disponibles	Valor por defecto
F1	Obtener ayuda	Ninguno	Ninguno
F2	Seleccionar el idioma de la instalación	Todos los idiomas admitidos	Inglés
F3	Cambiar la resolución de la pantalla para la instalación	• Modo de texto • VESA • resolución n.º 1 • resolución n.º 2 • ...	• El valor por defecto depende del hardware para gráficos instalado
F4	Seleccionar la fuente de la instalación	• CD-ROM/DVD • SLP • FTP • HTTP • NFS • SMB • Disco duro	CD-ROM/DVD
F5	Utilizar un disco de actualización para un controlador	Controlador	Ninguno

1.4.3 Uso de opciones de arranque personalizadas

El uso de las opciones de arranque adecuadas facilita el procedimiento de instalación. Muchos parámetros también pueden configurarse con posterioridad mediante las rutinas de linuxrc, pero el uso de opciones de arranque es más sencillo. En algunas configuraciones automáticas, las opciones de arranque pueden incorporarse con `initrd` o con un archivo `info`.

La siguiente tabla muestra las situaciones de instalación comentadas en el presente capítulo junto con los parámetros necesarios para el arranque y las correspondientes opciones de arranque. Simplemente añádalas en el orden que aparecen en la tabla para obtener una cadena de opciones de arranque que se pasará a las rutinas de instalación. Por ejemplo (en una sola línea):

```
install=... netdevice=... hostip=...netmask=... vnc=... vncpassword=...
```

Sustituya todos los valores (...) de la cadena con los valores correspondientes de su configuración.

Tabla 1.2 *Situaciones de instalación (arranque) descritas en este capítulo*

Situaciones de instalación	Parámetros necesarios para el arranque	Opciones de arranque
Capítulo *Instalación mediante YaST* (↑Inicio)	Ninguno: el sistema arranca automáticamente	No se necesita ninguna
Sección 1.1.1, “Instalación remota sencilla mediante VNC: configuración de red estática” (p. 18)	• Ubicación del servidor de la instalación • Dispositivo de red • Dirección IP • Máscara de red • Gateway • Habilitación de VNC	• `install=(nfs,http,ftp,smb)://via_a_mediosinst` • `netdevice=algun_dispositivo_de_red` (sólo es necesario si hay varios dispositivos de red disponibles) • `hostip=alguna_ip`

Situaciones de instalación	Parámetros necesarios para el arranque	Opciones de arranque
	• Contraseña de VNC	• `netmask=`*`alguna_mascara_de_red`* • `gateway=`*`gateway_ip`* • `vnc=1` • `vncpassword=`*`alguna_contraseña`*
Sección 1.1.2, “Instalación remota sencilla mediante VNC: configuración de red dinámica mediante DHCP” (p. 19)	• Ubicación del servidor de la instalación • Habilitación de VNC • Contraseña de VNC	• `install=(nfs,http,ftp,smb)://`*`via_a_mediosinst`* • `vnc=1` • `vncpassword=`*`alguna_contraseña`*
Sección 1.1.3, “Instalación remota mediante VNC: arranque en PXE y Wake on LAN” (p. 21)	• Ubicación del servidor de la instalación • Ubicación del servidor TFTP • Habilitación de VNC • Contraseña de VNC	No aplicable; el proceso se gestiona mediante PXE y DHCP
Sección 1.1.4, “Instalación remota sencilla mediante SSH: configuración de red estática” (p. 22)	• Ubicación del servidor de la instalación • Dispositivo de red • Dirección IP • Máscara de red • Gateway	• `install=(nfs,http,ftp,smb)://`*`via_a_mediosinst`* • `netdevice=`*`algun_dispositivo_de_red`* (sólo es necesario si hay varios dispositivos de red disponibles)

Situaciones de instalación	Parámetros necesarios para el arranque	Opciones de arranque
	• Habilitación de SSH • Contraseña SSH	• `hostip=`*`alguna_ip`* • `netmask=`*`alguna_mascara_de_red`* • `gateway=`*`gateway_ip`* • `usessh=1` • `sshpassword=`*`alguna_contraseña`*
Sección 1.1.5, “Instalación remota sencilla mediante SSH: configuración de red dinámica mediante DHCP” (p. 24)	• Ubicación del servidor de la instalación • Habilitación de SSH • Contraseña SSH	• `install=(nfs,http,ftp,smb)://`*`via_a_mediosinst`* • `usessh=1` • `sshpassword=`*`alguna_contraseña`*
Sección 1.1.6, “Instalación remota mediante SSH: arranque en PXE y Wake on LAN” (p. 25)	• Ubicación del servidor de la instalación • Ubicación del servidor TFTP • Habilitación de SSH • Contraseña SSH	No aplicable; el proceso se gestiona mediante PXE y DHCP

SUGERENCIA

Hay más información sobre las opciones de arranque de linuxrc que se utilizan para arrancar sistemas Linux en `/usr/share/doc/packages/linuxrc/linuxrc.html`.

1.5 Monitorización del proceso de instalación

Existen varias opciones para monitorizar de manera remota el proceso de instalación. Si se especifican las opciones de arranque adecuadas durante el arranque para la instalación, se puede utilizar VNC o bien SSH para controlar la instalación y la configuración del sistema desde una estación de trabajo remota.

1.5.1 Instalación de VNC

Mediante cualquier software para la visualización de VNC es posible controlar de forma remota la instalación de SUSE Linux desde prácticamente cualquier sistema operativo. En esta sección se describe la configuración cuando se utiliza una aplicación para la visualización de VNC o un navegador Web.

Preparación para la instalación con VNC

Todo lo que hay que hacer en el destino de la instalación para prepararlo para una instalación con VNC es incorporar las opciones de arranque correspondientes en el arranque para la instalación inicial (consulte la Sección 1.4.3, “Uso de opciones de arranque personalizadas” (p. 49)). El sistema de destino arranca en un entorno basado en texto y espera a que un cliente VNC se conecte al programa de instalación.

El programa de instalación muestra la dirección IP y el número de pantalla a los que es necesario conectarse para la instalación. Si se tiene acceso físico al sistema de destino, esta información se introduce inmediatamente después de que el sistema arranque para la instalación. Introduzca los datos cuando el software cliente VNC los solicite, así como la contraseña VNC.

Dado que el destino de la instalación se anuncia a sí mismo mediante OpenSLP, es posible obtener información de la dirección del destino de la instalación a través de un navegador SLP, sin necesidad de acceder físicamente a la instalación en sí, siempre y cuando la configuración de la red y todas las máquinas admitan OpenSLP:

1. Inicie el navegador de archivos y Web de KDE Konqueror.

2 Introduzca `service://yast.installation.suse` en la barra de direcciones.

El sistema de destino aparecerá como un icono en la pantalla de Konqueror. Al hacer clic en este icono se lanzará el visualizador de VNC de KDE, en el cual se realizará la instalación. También es posible ejecutar el software de visualización de VNC que prefiera con la dirección IP indicada y añadiendo `:1` al final de la dirección IP de la pantalla en la que se esté ejecutando la instalación.

Conexión al programa de instalación

Existen básicamente dos maneras de conectarse al servidor VNC (en este caso, el destino de la instalación). Es posible iniciar una aplicación para la visualización de VNC independiente en cualquier sistema operativo o bien conectarse mediante un navegador Web con Java habilitado.

Gracias a VNC es posible controlar la instalación de un sistema Linux desde cualquier otro sistema operativo, incluidas otras versiones de Linux, Windows y Mac OS.

En una máquina Linux, asegúrese de que el paquete `tightvnc` se encuentra instalado. En una máquina Windows, instale el puerto Windows de esta aplicación, que puede obtenerse en la página principal de TightVNC (`http://www.tightvnc.com/download.html`).

Para conectarse al programa de instalación que se ejecuta en la máquina de destino, siga estos pasos:

1 Inicie el visualizador de VNC.

2 Introduzca la dirección IP y el número de pantalla del destino de la instalación ofrecido por el navegador SLP o por el propio programa de instalación.

`dirección_ip:numero_de_pantalla`

Se abrirá una ventana en el escritorio con las pantallas de YaST como en una instalación local normal:

El uso de un navegador Web para conectarse al programa de instalación evita la dependencia de un software de VNC y del sistema operativo en el que se ejecute. Es posible utilizar cualquier navegador (Firefox, Konqueror, Internet Explorer, Opera etc.)

para realizar la instalación del sistema Linux, con tal de que la aplicación de navegación tenga Java habilitado.

Siga este procedimiento para realizar una instalación VNC:

1. Inicie el navegador Web que prefiera.
2. Introduzca lo siguiente como dirección:

   `http://ip_address_of_target:5801`

3. Introduzca la contraseña de VNC cuando se le pida. La ventana del navegador mostrará las pantallas de YaST como en una instalación local normal.

1.5.2 Instalación con SSH

Gracias a SSH, es posible controlar de forma remota la instalación de la máquina Linux mediante cualquier software cliente de SSH.

Preparación para la instalación con SSH

Aparte de la instalación de los paquetes de software correspondientes (OpenSSH para Linux y PuTTY para Windows), sólo es necesario pasar las opciones de arranque apropiadas para habilitar SSH para la instalación. Para obtener más información, consulte la Sección 1.4.3, “Uso de opciones de arranque personalizadas” (p. 49). OpenSSH se instala por defecto en todos los sistemas operativos basados en SUSE Linux.

Conexión al programa de instalación

1. Obtenga la dirección IP del destino de la instalación.

   Si se tiene acceso físico a la máquina de destino, utilice la dirección IP que las rutinas de instalación muestran en la consola tras el arranque inicial. También es posible tomar la dirección IP asignada a este host en particular en la configuración del servidor DHCP.

2. En la línea de comandos, introduzca el comando siguiente:

   `ssh -X root@ip_address_of_target`

Sustituya *dirección_ip_del_destino* por la dirección IP real del destino de la instalación.

3 Cuando se pida un nombre de usuario, introduzca `root`.

4 Cuando se pida una contraseña, introduzca la contraseña establecida mediante la opción de arranque de SSH.

Una vez realizada correctamente la autenticación, aparecerá un indicador de línea de comandos correspondiente al destino de la instalación.

5 Introduzca `yast` para iniciar el programa de instalación.

Se abrirá una ventana que mostrará las pantallas normales de YaST como se describe en el Capítulo *Instalación mediante YaST* (↑Inicio).

2 Configuración avanzada de disco

Las configuraciones avanzadas del sistema requieren configuraciones de disco concretas. Para que la denominación de los dispositivos sea coherente con la de los dispositivos SCSI, utilice un guión de inicio específico o udev. La LVM (Gestión lógica de volúmenes) es un esquema de partición de discos diseñado para ser mucho más flexible que la partición física utilizada en las configuraciones estándar. Su funcionalidad de instantáneas permite crear de forma sencilla copias de seguridad de los datos. La matriz redundante de discos independientes (RAID, del inglés Redundant Array of Independent Disks) ofrece niveles superiores de integridad de los datos, rendimiento y tolerancia a fallos.

2.1 Configuración de LVM

En esta sección se describen brevemente los principios sobre los que se asienta LVM y las funciones básicas que lo hacen útil en muchas circunstancias. En la Sección 2.1.2, “Configuración de LVM con YaST” (p. 60), aprenderá a configurar LVM con YaST.

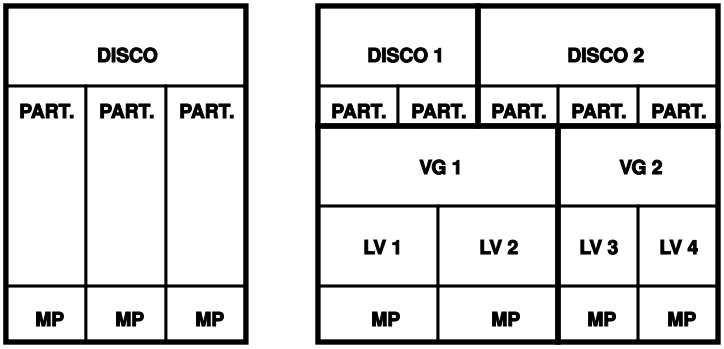
AVISO

El uso de LVM podría asociarse con un aumento del riesgo, por ejemplo, de pérdida de datos. Otros riesgos posibles incluirían la detención de las aplicaciones por fallo, fallos de alimentación y comandos erróneos. Haga una copia de seguridad de los datos antes de implementar LVM o volver a configurar los volúmenes. Nunca haga nada sin haber hecho antes una copia de seguridad.

2.1.1 Administrador de volúmenes lógicos

El Administrador de volúmenes lógicos (LVM) permite la distribución flexible del espacio del disco duro en varios sistemas de archivos. Se desarrolló porque, en ocasiones, surge la necesidad de cambiar la segmentación del disco duro después de hacer la partición inicial que se realiza durante la instalación. Puesto que es difícil modificar las particiones en un sistema que se está ejecutando, LVM ofrece un repositorio virtual (grupo de volúmenes, VG en adelante por sus siglas en inglés) de espacio en memoria desde el que se pueden crear los volúmenes lógicos (LV) según sea necesario. El sistema operativo accede a estos LV en lugar de a particiones físicas. Los grupos de volúmenes pueden prolongarse a más de un disco, de manera que varios discos o partes de ellos puedan formar un único VG. De esta forma, LVM ofrece un tipo de abstracción a partir del espacio de disco físico que permite cambiar la segmentación de una manera más sencilla y segura que hacer una partición física. Encontrará información básica relativa a la particiones físicas en la sección “Tipos de partición” (Capítulo 1, *Instalación mediante YaST*, ↑Inicio) y en la Sección “Particionamiento” (Capítulo 2, *Configuración del sistema con YaST*, ↑Inicio).

Figura 2.1 *Particiones físicas y LVM*



En la Figura 2.1, “Particiones físicas y LVM” (p. 58) se compara una partición física (a la izquierda) con una segmentación de LVM (a la derecha). En la parte izquierda, se ha dividido un disco en tres particiones físicas (PARTE), cada uno con un punto de montaje (PM) asignado de manera que el sistema operativo pueda acceder a ellos. En la parte derecha, hay dos discos divididos en dos o tres particiones físicas cada uno. Se han definido dos grupos de volúmenes de LVM (VG 1 y VG 2). VG 1 contiene dos particiones del DISCO 1 y una del DISCO 2. VG 2 contiene las dos particiones restantes del DISCO 2. En LVM, las particiones físicas del disco que se incorporan a un grupo

de volúmenes se denominan "volúmenes físicos". En los grupos de volúmenes, se han definidos cuatro volúmenes lógicos (LV 1 a LV 4), que el sistema operativo podrá utilizar gracias a los puntos de montaje asociados. El límite entre volúmenes lógicos diferentes no tiene por qué alinearse con ningún borde de la partición. Observe en este ejemplo el borde entre LV 1 y LV 2.

Funciones de LVM:

- Es posible combinar varios discos duros o particiones en un volumen lógico de gran tamaño.
- Siempre que la configuración sea adecuada, se puede aumentar de tamaño un LV (como `/usr`) cuando ya no quede espacio libre.
- Mediante LVM, incluso se pueden añadir discos duros o LV en un sistema en funcionamiento. No obstante, para ello es necesario un hardware de intercambio directo que sea capaz de realizar dichas acciones.
- Es posible activar un "modo de repartición" que distribuya el flujo de datos de un volumen lógico en varios volúmenes físicos. Si estos volúmenes físicos residen en discos distintos, mejorará el rendimiento de los procesos de lectura y escritura, como ocurre en RAID 0.
- La función de instantánea permite realizar copias de seguridad coherentes (especialmente para servidores) en el sistema en funcionamiento.

Con estas funciones, el uso de LVM sí tiene sentido para equipos domésticos que soporten una gran carga de trabajo o pequeños servidores. Si cuenta con una cantidad de datos cada vez mayor, como en el caso de las bases de datos, archivos de reserva de música o directorios de usuario, LVM es, sin duda, lo más adecuado, ya que permite sistemas de archivos que ocupan más que el disco duro. Otra ventaja de LVM es que se pueden añadir hasta 256 LV. Sin embargo, tenga en cuenta que trabajar con LVM es distinto a trabajar con particiones convencionales. Hay más información disponible e instrucciones acerca de cómo configurar LVM en la página oficial de LVM HOWTO en `http://tldp.org/HOWTO/LVM-HOWTO/`.

A partir de la versión 2.6 del núcleo, está disponible la versión 2 de LVM, que a su vez, es compatible con las versiones anteriores de LVM y permite la gestión continua de los grupos de volúmenes antiguos. Al crear nuevos grupos de volúmenes, decida si desea usar el formato nuevo o la versión compatible con versiones anteriores. LVM 2 no necesita ninguna revisión del núcleo ya que usa el asignador de dispositivos integrado

en el núcleo 2.6. Este núcleo sólo es compatible con la versión 2 de LVM. Por lo tanto, cuando en esta sección se haga referencia a LVM, se estará refiriendo a la versión 2.

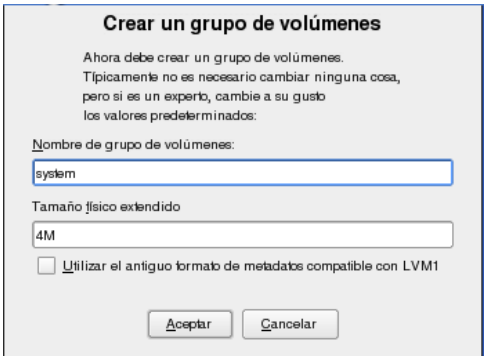
2.1.2 Configuración de LVM con YaST

Con la herramienta de particionamiento en modo experto de YaST se puede configurar LVM con YaST (consulte la Sección “Particionamiento” (Capítulo 2, *Configuración del sistema con YaST*, ↑Inicio)). Esta herramienta permite editar y suprimir las particiones existentes y crear otras nuevas para que se utilicen con LVM. Con ella, para crear una partición LVM, primero se debe hacer clic en *Crear* → *No formatear* y seleccionar a continuación *0x8E Linux LVM* como identificador de la partición. Una vez creadas las particiones que se van a usar con LVM, se hace clic en *LVM* para iniciar la configuración.

Creación de grupos de volúmenes

Si no existe todavía ningún grupo de volúmenes en el sistema, se le pedirá que añada uno (consulte la Figura 2.2, “Creación de un grupo de volúmenes” (p. 60)). Es posible crear grupos adicionales con *Añadir grupo* pero, por lo general, es suficiente un sólo grupo de volúmenes. Se sugiere `system` como nombre para el grupo de volúmenes en el que se encuentren los archivos de sistema de SUSE Linux. El tamaño de extensión física define el tamaño de un bloque físico en el grupo de volúmenes. Todo el espacio en disco de un grupo de volúmenes se gestionará en porciones de este tamaño. El valor se define normalmente en 4 MB y se permite un tamaño máximo de 256 GB para volúmenes físicos y lógicos. Sólo debería aumentarse el tamaño de extensión física, por ejemplo, a 8, 16 o 32 MB, si necesita volúmenes lógicos más grandes que 256 GB.

Figura 2.2 *Creación de un grupo de volúmenes*

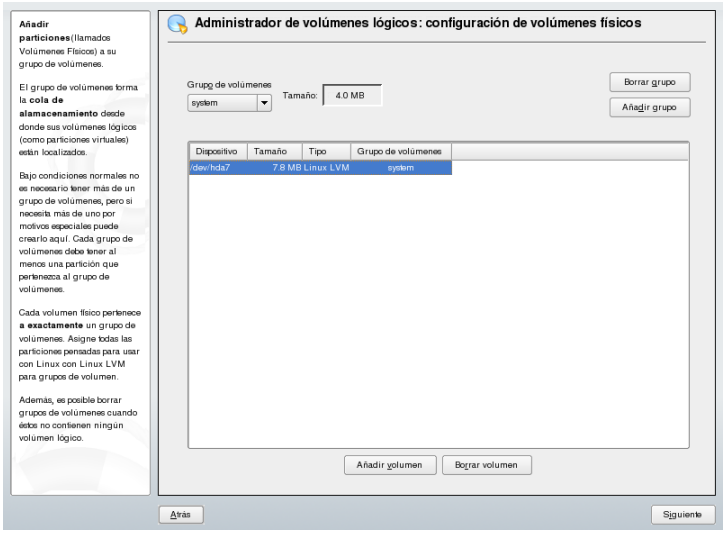


Configuración de los volúmenes físicos

Después de crear el grupo de volúmenes, el cuadro de diálogo siguiente recoge todas las particiones, ya sean del tipo “Linux LVM” o “Linux nativo”. No se muestran intercambios ni particiones DOS. Si ya se ha asignado una partición a un grupo de volúmenes, el nombre del grupo aparecerá en la lista. Las particiones no asignadas se indican con “--”.

Si hay varios grupos de volúmenes, defina el actual en el cuadro de selección situado en la parte superior izquierda. Los botones de la parte superior derecha habilitan la creación de grupos de volúmenes adicionales y la supresión de los existentes. Solamente se pueden suprimir aquellos grupos de volúmenes que no tengan particiones asignadas. Las particiones asignadas a un grupo de volúmenes también se denominan "volúmenes físicos".

Figura 2.3 *Configuración del volumen físico*



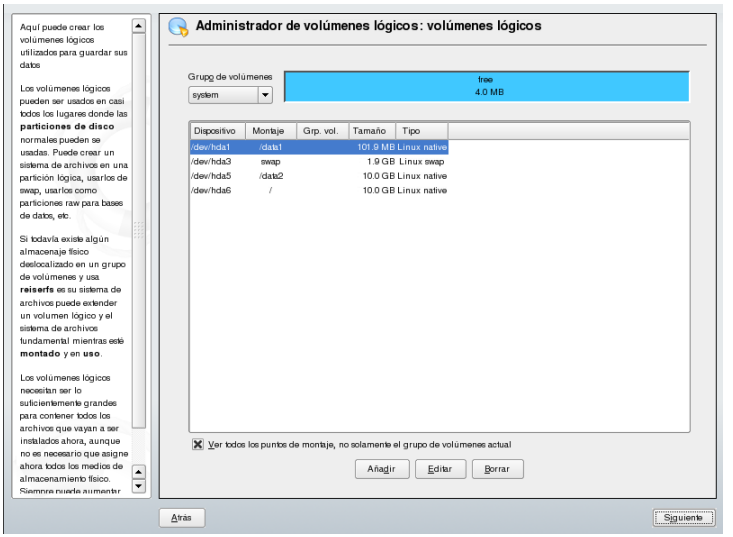
Para añadir una partición no asignada previamente al grupo de volúmenes seleccionado, haga clic primero en la partición y, a continuación, en *Añadir volumen.* En este momento, el nombre del grupo de volúmenes se introduce al lado de la partición seleccionada. Asigne todas las particiones reservadas a LVM a un grupo de volúmenes. De lo contrario, el espacio de la partición permanecerá inutilizado. Antes de salir del cuadro de diálogo, debe asignarse al menos cada grupo de volúmenes a un volumen físico. Después de

asignar todos los volúmenes físicos, haga clic en *Siguiente* para seguir con la configuración de los volúmenes lógicos.

Configuración de los volúmenes lógicos

Después de que el grupo de volúmenes se haya llenado de volúmenes físicos, defina los volúmenes lógicos que el sistema operativo debería usar en el siguiente cuadro de diálogo. Establezca el grupo de volúmenes actual en el cuadro de selección situado en la parte superior izquierda. A su lado se mostrará el espacio libre que queda en el grupo de volúmenes actual. La lista que aparece a continuación contiene los volúmenes lógicos en ese grupo de volúmenes. Aquí se muestran las particiones normales de Linux a las que se ha asignado un punto de montaje, las de intercambio y todos los volúmenes lógicos existentes. *Añada, edite* o *elimine* los volúmenes lógicos según sea necesario hasta que ya no quede espacio en el grupo de volúmenes. Asigne al menos un volumen lógico a cada grupo de volúmenes.

Figura 2.4 *Gestión de volúmenes lógicos*



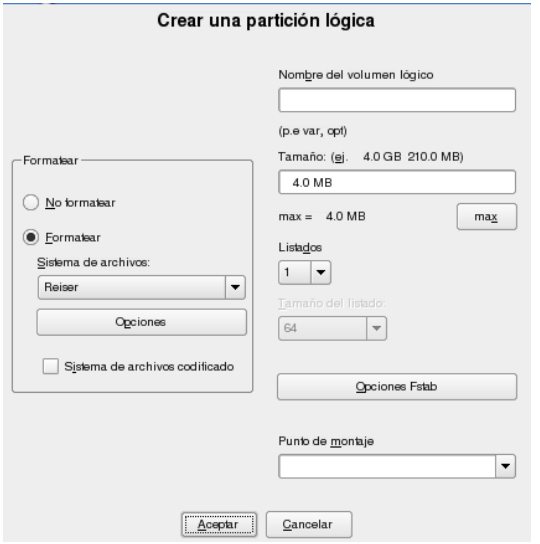
Para crear un nuevo volumen lógico, haga clic en *Añadir* y complete el mensaje emergente que se abre. Al igual que ocurre con las particiones, introduzca el tamaño, el sistema de archivos y el punto de montaje. Normalmente, los sistemas de archivos, como reiserfs o ext2, se crean en un volumen lógico y, a continuación, se designa un punto de montaje. Los archivos almacenados en este volumen lógico pueden encontrarse

en este punto de montaje en el sistema instalado. También es posible distribuir el flujo de datos en el volumen lógico entre varios volúmenes físicos (repartición). Si estos volúmenes físicos residen en discos duros distintos, por lo general se mejorará el rendimiento de los procesos de lectura y escritura (como en RAID 0). Por contra, un LV de repartición con n reparticiones sólo se podrá crear correctamente si el espacio en disco duro que necesita el LV se puede distribuir uniformemente en n volúmenes físicos. Si, por ejemplo, únicamente hay dos volúmenes físicos disponibles, será imposible crear un volumen lógico con tres reparticiones.

AVISO: Repartición de datos

YaST no tiene posibilidad en este punto de comprobar si son correctas las entradas que tienen que ver con la repartición. Cualquier error que se haya cometido aquí sólo será obvio más tarde, cuando LVM se implemente en el disco.

Figura 2.5 *Creación de volúmenes lógicos*



Si ya ha configurado LVM en el sistema, ya podrán introducirse los volúmenes lógicos existentes. Antes de continuar, asigne también puntos de montaje adecuados a estos volúmenes lógicos. Si hace clic en *Siguiente,* volverá al particionamiento en modo experto de YaST y terminarán ahí sus operaciones.

Gestión directa de LVM

Si ya ha configurado LVM y sólo desea cambiar algún elemento, existe una manera alternativa de hacerlo. En el Centro de control de YaST, seleccione *Sistema → LVM*. Este cuadro de diálogo permite básicamente las mismas acciones descritas anteriormente, con la excepción del particionamiento físico. Muestra los volúmenes físicos y lógicos existentes en dos listas. Podrá gestionar el sistema LVM mediante los métodos ya descritos.

2.2 Configuración de RAID de software

El propósito de RAID (Redundant Array of Independent Disks, Formación redundante de discos independientes) es combinar varias particiones de disco duro en un disco duro *virtual* para optimizar el rendimiento, la seguridad de los datos o ambas cosas. La mayoría de controladores RAID utilizan el protocolo SCSI porque llega a un número mayor de discos duros de un modo más eficaz que el protocolo IDE y es más adecuado para el procesamiento paralelo de comandos. Hay algunos controladores RAID que admiten discos duros IDE o SATA. El software RAID ofrece las ventajas de los sistemas RAID, pero sin el coste adicional de los controladores de hardware RAID. Sin embargo, esto supone tiempo de la CPU y exige unos requisitos de memoria que lo hace inadecuado para equipos con un rendimiento real alto.

2.2.1 Niveles de RAID

SUSE Linux ofrece la opción de combinar varios discos duros en un sistema RAID de software con la ayuda de YaST: una alternativa muy razonable al RAID de hardware. RAID implica varias estrategias para combinar varios discos duros en un sistema RAID, cada una de las cuales tiene diferentes objetivos, ventajas y características. Las variaciones se denominan normalmente *niveles de RAID*.

Los niveles normales de RAID son:

RAID 0
: Este nivel mejora el rendimiento del acceso a los datos difundiendo los bloques de cada archivo por varias unidades de disco. En realidad, no se trata de un RAID,

porque no proporciona copias de seguridad de los datos, pero el nombre *RAID 0* para este tipo de sistema se ha convertido en la norma. Con RAID 0, se agrupan dos o más discos duros. El rendimiento es muy bueno, pero el sistema RAID se destruye y los datos se pierden sólo con que falle un disco duro.

RAID 1

Este nivel proporciona una seguridad adecuada para los datos, porque éstos se copian en otro disco duro 1:1. Esto se denomina *copia de discos duros en espejo*. Si se destruye un disco, se podrá conseguir una copia de su contenido en otro. Todos ellos excepto uno podrían resultar dañados sin poner los datos en peligro. Sin embargo, si no se detecta ningún daño, también puede ocurrir que los datos dañados estén duplicados en el disco correcto y que el daño en los datos provenga de ahí. La velocidad de escritura es un poco menor en el proceso de copia en comparación con el acceso a un único disco (de diez a veinte por ciento más lento), pero el acceso de lectura es notablemente más rápido con respecto a uno de los discos duros físicos normales, porque los datos se duplican de modo que se pueden escanear de forma paralela. En general, se puede decir que el nivel 1 proporciona casi el doble de velocidad de lectura y casi la misma velocidad de escritura de discos únicos.

RAID 2 y RAID 3

Éstas no son implementaciones típicas de RAID. El nivel 2 distribuye los datos por bits en lugar de por bloques. El nivel 3 reparte los datos por bytes con un disco de paridad dedicado y no puede ocuparse de varias peticiones a la vez. Los dos niveles no se utilizan casi nunca.

RAID 4

El nivel 4 distribuye los datos por bloques, como el nivel 0 combinado con un disco de paridad dedicado. En caso de que el disco de datos falle, se crea un disco de sustitución con los datos de paridad. Sin embargo, el disco de paridad puede obstaculizar el acceso de escritura. No obstante, el nivel 4 se utiliza a veces.

RAID 5

El RAID 5 es un compromiso optimizado entre el Nivel 0 y el Nivel 1 en cuanto a rendimiento y seguridad de los datos. Un espacio de disco duro equivale al número de discos utilizados menos uno. Los datos se distribuyen por los discos duros como con RAID 0. Los *bloques de paridad*, creados en una de las particiones, tienen como finalidad proporcionar la seguridad. Se enlazan entre sí con XOR, lo que permite que el bloque de paridad correspondiente reconstruya el contenido en caso de que se produzca un error en el sistema. Con RAID 5, no puede fallar más de un

disco duro a la vez. Si un disco duro falla, debe sustituirse en cuanto sea posible para evitar el riesgo de perder datos.

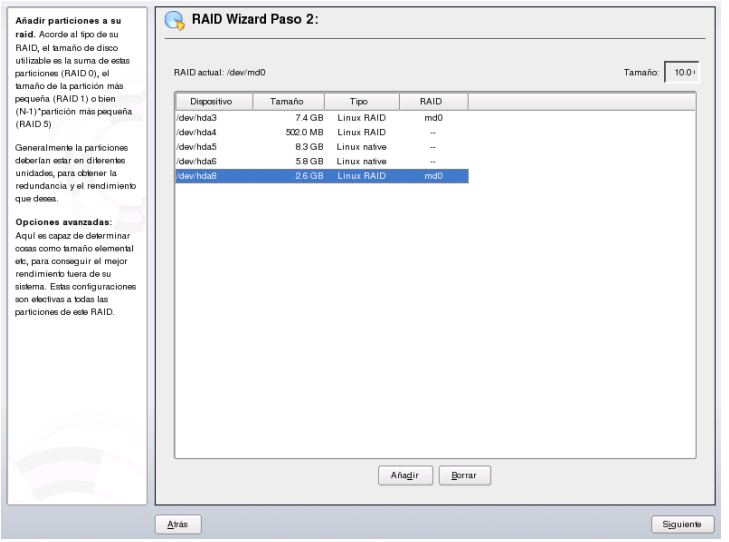
Otros niveles de RAID
: Se han desarrollado algunos otros niveles de RAID (RAIDn, RAID 10, RAID 0+1, RAID 30, RAID 50, etc.), algunos de los cuales son implementaciones creadas por proveedores de hardware con derechos de propiedad. Estos niveles no están muy extendidos, de modo que no se explican aquí.

2.2.2 Configuración de RAID de software con YaST

Desde la herramienta de particionamiento en modo avanzado de YaSt, se puede llegar a la configuración de RAID de software con YaST, como se describe en la Sección "Particionamiento" (Capítulo 2, *Configuración del sistema con YaST*, ↑Inicio). Esta herramienta de particionamiento le permite editar y suprimir las particiones existentes y crear otras nuevas para que se utilicen con el software RAID. Con ella, puede crear particiones RAID: haga clic en *Crear* → *No formatear* y, a continuación, seleccione *0xFD Linux RAID* como identificador de la partición. Para RAID 0 y RAID 1, se necesitan al menos dos particiones: para RAID 1, suelen ser exactamente dos. Si se utiliza RAID 5, se necesitan al menos tres particiones. Se recomienda tomar sólo particiones del mismo tamaño. Las particiones RAID deberían almacenarse en discos duros diferentes para disminuir el riesgo de perder datos si una de ellas no es correcta (RAID 1 y 5) y para optimizar el rendimiento de RAID 0. Después de crear todas las particiones que se van a utilizar con RAID, haga clic en *RAID* → *Crear RAID* para iniciar la configuración de RAID.

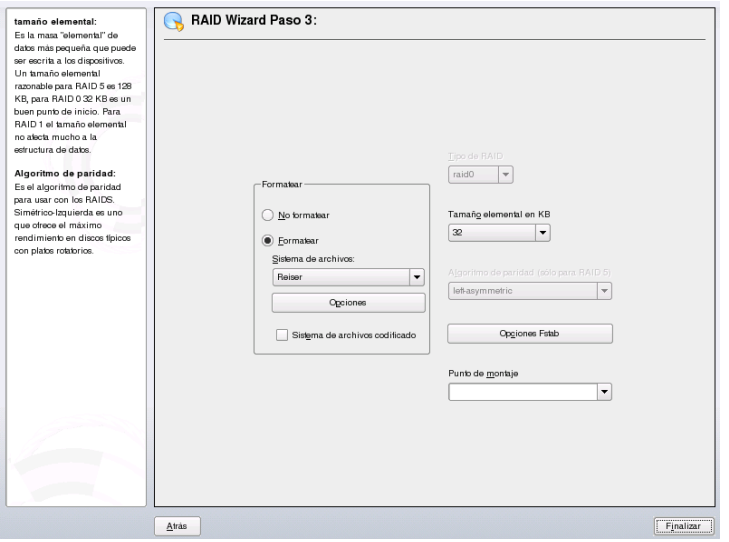
En el cuadro de diálogo siguiente, elija entre los niveles de RAID 0, 1 y 5 (para obtener más información, consulte la Sección 2.2.1, "Niveles de RAID" (p. 64)). Al hacer clic en *Siguiente*, el siguiente cuadro de diálogo muestra todas las particiones del tipo "Linux RAID" o "Linux native" (consulte la Figura 2.6, "Particiones RAID" (p. 67)). No se muestran intercambios ni particiones DOS. Si ya se ha asignado una partición a un volumen de RAID, el nombre del dispositivo RAID (por ejemplo, `/dev/md0`) aparece en la lista. Las particiones no asignadas se indican con "--".

Figura 2.6 *Particiones RAID*



Para añadir una partición no asignada previamente al volumen RAID seleccionado, haga clic primero en la partición y, a continuación, en *Añadir*. En este momento, el nombre del dispositivo RAID se introduce al lado de la partición seleccionada. Asigne todas las particiones reservadas para RAID. De lo contrario, el espacio de la partición permanecerá inutilizado. Después de asignar todas las particiones, haga clic en *Siguiente* para continuar con el cuadro de diálogo de configuración en el que puede definir de un modo más preciso el rendimiento (consulte la Figura 2.7, “Configuración del sistema de archivos” (p. 68)).

Figura 2.7 *Configuración del sistema de archivos*



Al igual que el particionamiento convencional, configure el sistema de archivos por utilizar y la codificación y el punto de montaje del volumen RAID. La selección de *Superbloque persistente* garantiza que las particiones RAID se reconozcan como tal al arrancar. Después de completar la configuración con *Finalizar*, compruebe el dispositivo `/dev/md0` y los demás indicados con *RAID* en el particionamiento en modo avanzado.

2.2.3 Solución de problemas

Compruebe el archivo `/proc/mdstats` para ver si se ha destruido una partición RAID. En caso de que el sistema falle, apague el sistema Linux y sustituya el disco duro por uno nuevo particionado del mismo modo. A continuación, reinicie el sistema e introduzca el comando `mdadm /dev/mdX --add /dev/sdX`. Sustituya "X" por sus propios identificadores de dispositivos. Esto integra el disco duro de forma automática en el sistema RAID y lo reconstruye completamente.

2.2.4 Información adicional

Las instrucciones de configuración y más información acerca del RAID de software se pueden encontrar en las ayudas en:

- `/usr/share/doc/packages/raidtools/Software-RAID.HOWTO.html`
- `http://en.tldp.org/HOWTO/Software-RAID-HOWTO.html`

También están disponibles listas de correo de Linux RAID, como `http://marc.theaimsgroup.com/?l=linux-raid&r=1&w=2`.

Actualización del sistema y gestión de paquetes

3

SUSE Linux ofrece la opción de actualizar un sistema existente sin tener que volver a instalarlo por completo. Hay dos tipos de actualizaciones: *actualización de paquetes de software individuales* y *actualización del sistema completo.* Los paquetes también se pueden instalar manualmente con el gestor de paquetes RPM.

3.1 Actualización de SUSE Linux

El software tiende a "crecer" de una versión a la siguiente. Por ello, antes de actualizar debe saber de cuánto espacio dispone en la partición, empleando para ello el comando `df`. Si sospecha que no dispone de mucho espacio en el disco, asegure los datos antes de actualizar el sistema y volver a partirlo. No existe ninguna regla general sobre cuánto espacio tiene que tener cada partición. Los requisitos en materia de espacio dependen del perfil particular de particionamiento, el software seleccionado y el número de la versión de SUSE Linux.

3.1.1 Preparación

Antes de actualizar, para asegurar los datos copie los archivos de configuración antiguos en otro medio, como un lector de cintas magnéticas, un disco duro extraíble, un dispositivo de almacenamiento USB stick o una unidad ZIP. Esta recomendación se aplica fundamentalmente a los archivos almacenados en `/etc`, además de a algunos directorios y archivos de `/var` y `/opt`. También puede ser conveniente escribir los datos de usuario del directorio `/home` (los directorios `HOME`) en un medio de copia de

seguridad. Haga una copia de seguridad de estos datos como usuario `Root.` Sólo los usuarios `Root` disponen de permiso de escritura para todos los archivos locales.

Antes de empezar el proceso de actualización, anote la partición raíz. El comando `df /` indica el nombre de dispositivo de la partición raíz. En el Ejemplo 3.1, “Lista con `df -h`” (p. 72), la partición raíz que se debe escribir es `/dev/hda3` (montada como `/`).

Ejemplo 3.1 *Lista con df -h*

```
Filesystem     Size  Used Avail Use% Mounted on
/dev/hda3       74G   22G   53G  29% /
tmpfs          506M     0  506M   0% /dev/shm
/dev/hda5      116G  5.8G  111G   5% /home
/dev/hda1       39G  1.6G   37G   4% /windows/C
/dev/hda2      4.6G  2.6G  2.1G  57% /windows/D
```

3.1.2 Problemas posibles

Si actualiza un sistema por defecto de la versión anterior a esta, YaST calcula cuáles son los cambios necesarios y los ejecuta. Dependiendo de las personalizaciones que se lleven a cabo, algunos pasos del procedimiento de actualización completo podrían fallar, o puede que finalmente tenga que recuperar los datos de la copia de seguridad efectuada. Apuntamos aquí una serie de puntos más que deben comprobarse antes de iniciar la actualización del sistema.

Comprobación de los archivos passwd y group en /etc

Antes de actualizar el sistema, compruebe que `/etc/passwd` y `/etc/group` no contengan errores de sintaxis. Para ello, inicie las utilidades de verificación `pwck` y `grpck` como usuario `Root` y elimine los errores que aparezcan.

PostgreSQL

Antes de actualizar PostgreSQL `(postgres),` vuelque la base de datos. Consulte la página Man de `pg_dump`. Esto sólo es necesario si se utilizó PostgreSQL antes de actualizar.

3.1.3 Actualización con YaST

Ahora podrá actualizar el sistema siguiendo el procedimiento de preparación resumido en la Sección 3.1.1, “Preparación” (p. 71):

1. Arranque el sistema como si fuera a instalar, tal y como se describe en la Sección “Preparación del sistema para la instalación” (Capítulo 1, *Instalación mediante YaST*, ↑Inicio). En YaST, elija un idioma y seleccione *Actualizar* en el cuadro de diálogo *Modo de instalación.*. No seleccione *Nueva instalación.*

2. YaST determina si hay varias particiones raíz o no. Si sólo hay una, proceda con el paso siguiente. Si hay varias, seleccione la partición adecuada y confirme con *Siguiente* (en el ejemplo de la Sección 3.1.1, “Preparación” (p. 71) se seleccionó `/dev/hda3`). YaST lee el archivo `fstab` antiguo de la partición para analizar y montar los sistemas de archivos listados aquí.

3. En el cuadro de diálogo *Configuración de la instalación,* ajuste los valores según convenga. Se pueden dejar los ajustes por defecto tal cual, pero si quiere mejorar el sistema, examine los paquetes que se ofrecen en los submenús *Selección de software* o añada compatibilidad con otros idiomas.

   También puede hacer más copias de seguridad de varios componentes del sistema. La selección de copias de seguridad hace más lento el proceso de actualización. Utilice esta opción si no dispone de una copia de seguridad reciente del sistema.

4. En el cuadro de diálogo que sigue, seleccione actualizar sólo el software ya instalado o añadir componentes de software nuevos al sistema (modo de actualización). Se recomienda aceptar la combinación sugerida, por ejemplo *Actualización basada en la sección "Sistema estándar con KDE"* o *"Sistema estándar con GNOME"*. Podrá realizar ajustes más adelante con YaST.

3.1.4 Actualización de paquetes individuales

Independientemente del entorno global actualizado, siempre puede actualizar paquetes individualmente. Desde este punto en adelante, no obstante, es su responsabilidad garantizar que el sistema permanezca coherente. En `http://www.novell.com/linux/download/updates/` encontrará algunas sugerencias en cuanto a actualización.

Seleccione los componentes oportunos en la lista de selección de paquetes de YaST. Si selecciona un paquete esencial para el funcionamiento global del sistema, YaST emitirá una advertencia. Estos paquetes sólo se deben actualizar en el modo de actualización. Por ejemplo, muchos paquetes contienen *bibliotecas compartidas.* Si actualiza estos programas y estas aplicaciones cuando el sistema se está ejecutando, pueden producirse problemas.

3.2 Cambios de software de versión a versión

A continuación se detallan los aspectos individuales modificados de una versión a otra. Este resumen indica, por ejemplo, si los ajustes básicos se han vuelto a configurar por completo, si los archivos de configuración se han desplazado a otros lugares o si han cambiado significativamente las aplicaciones comunes. A continuación se tratan las modificaciones que afectan significativamente al uso diario del sistema, bien a nivel de usuario, bien a nivel de administrador.

A medida que se van identificando problemas y situaciones especiales sobre las distintas versiones, se van publicando en línea. Consulte los enlaces incluidos a continuación. En `http://www.novell.com/products/linuxprofessional/downloads/` encontrará importantes actualizaciones para paquetes individuales. Para acceder a estas actualizaciones deberá utilizar YaST Online Update (YOU). Consulte la Sección "Actualización del software en línea" (Capítulo 2, *Configuración del sistema con YaST*, ↑Inicio).

3.2.1 De la 9.0 a la 9.1

Consulte el artículo "Known Problems and Special Features in SUSE Linux 9,1" (Problemas conocidos y funciones especiales en SUSE Linux 10), en la base de datos de asistencia de SUSE en `http://portal.suse.com`, bajo la palabra clave *special features* (funciones especiales). Estos artículos se publican nuevos en cada versión de SUSE Linux.

Actualización a la versión 2.6 del núcleo

SUSE Linux se basa ahora por completo en el núcleo 2.6. La versión anterior (2.4) ya no se puede seguir utilizando, ya que las aplicaciones adjuntas no funcionan con el núcleo 2.4. Tenga en cuenta los siguientes detalles:

- Los carga de módulos se configura mediante el archivo `/etc/modprobe.conf`. El archivo `/etc/modules.conf` ha quedado obsoleto. YaST intentará convertir el archivo (consulte también el guión `/sbin/generate-modprobe.conf`).
- Los módulos llevan el sufijo `.ko`.
- Ya no hace falta el módulo `ide-scsi` para grabar discos CD.
- El prefijo `snd_` se ha eliminado de las opciones del módulo de sonido ALSA.
- `sysfs` complementa ahora el sistema de archivos `/proc`.
- Se ha mejorado el sistema de gestión de energía (especialmente ACPI), y ahora se puede configurar con un módulo de YaST.

Montaje de particiones VFAT

A la hora de montar particiones VFAT, es necesario cambiar el parámetro `code` a `codepage`. Si tiene problemas a la hora de montar una partición VFAT, compruebe si el archivo `/etc/fstab` contiene el nombre del parámetro antiguo.

Stand-by y suspensión con ACPI

La versión 2.6 del núcleo es compatible con el sistema de stand-by y suspensión con ACPI. Esta función se encuentra aún en fase experimental y puede no ser compatible con algunos componentes de hardware. Para utilizarla necesitará el paquete `powersave`. Hay más información disponible sobre este paquete en `/usr/share/doc/packages/powersave`. Dispone de una interfaz de usuario gráfica en el paquete `kpowersave`.

Dispositivos de entrada

Independientemente de los cambios en cuanto a los dispositivos de entrada, consulte el artículo anteriormente mencionado “Known Problems and Special Features in SUSE LINUX 9.1” (Problemas conocidos y funciones especiales en SUSE Linux 9.1), en la base de datos de asistencia en `http://portal.suse.com`, bajo la palabra clave *special features* (funciones especiales).

Biblioteca de hilos POSIX nativa y glibc 2.3.x

Las aplicaciones vinculadas a NGPT (tratamiento de hilos POSIX de siguiente generación) no funcionan con glibc 2.3.x. Todas las aplicaciones afectadas que no acompañan a SUSE Linux deben compilarse con linuxthreads o con NPTL (biblioteca de hilos POSIX nativa). Es preferible utilizar NPTL, ya que será el estándar en el futuro.

Si NPTL genera dificultades, se pueden implementar linuxthreads antiguos definiendo la siguiente variable de entorno (sustituya *`versión-núcleo`* por el número de la versión del núcleo en cuestión):

```
LD_ASSUME_KERNEL=versión-núcleo
```

Estos son los números de versión posibles:

2.2.5 (i386 e i586):
: linuxthreads sin stacks flotantes

2.4.1 (AMD64, IPF, s390x, i586, i686):, 2.4.1 (AMD64, i586 e i686):
: linuxthread con stacks flotantes

Notas relacionadas con el núcleo y con linuxthreads con stacks flotantes: las aplicaciones que utilizan `errno, h_errno` y `_res` deben incluir los archivos de encabezado (`errno.h, netdb.h` y `resolv.h`) con `#include`. En el caso de programas C++ con compatibilidad con varios hilos que emplean la *cancelación de hilos,* debe utilizarse la variable de entorno `LD_ASSUME_KERNEL=2.4.1` para solicitar el uso de la biblioteca de linuxthreads.

Adaptaciones para la *biblioteca de hilos POSIX nativa*

NPTL viene incluido en SUSE Linux 9.1 como paquete de hilos. NPTL es compatible en binarios con la antigua biblioteca de linuxthreads. No obstante, en las áreas en las

que linuxthreads no cumpla con el estándar POSIX será necesario adaptar la biblioteca NPTL. Ello incluiría: gestión de señales, devolución del mismo valor por parte de `getpid` en todos los hilos y gestores de hilos registrados con pthread_atfork que no funcionan al utilizar `vfork.`

Configuración de interfaces de red

La configuración de la interfaz de red ha cambiado. Antes, el hardware se iniciaba siguiendo la configuración de una interfaz que no existía. Ahora, el sistema busca el nuevo hardware y lo inicia de forma inmediata permitiendo configurar la nueva interfaz de red.

Se han introducido nombres nuevos en los archivos de configuración. Dado que los nombres de las interfaces de red se generan automáticamente y cada vez se utilizan más dispositivos HotPlug, nombres como `eth0` o `eth1` han dejado de ser adecuados por motivos de configuración. Por esta razón se usan designaciones únicas como la dirección MAC o la ranura PCI para dar nombre a las configuraciones de interfaces. Puede utilizar los nombres de interfaz en cuanto aparezcan. Todavía se pueden emplear comandos como `ifup eth0` o `ifdown eth0`.

Las configuraciones de los dispositivos se encuentran en `/etc/sysconfig/hardware.` Las interfaces provistas con estas configuraciones se suelen ubicar en `/etc/sysconfig/network` (con diferentes nombres). Consulte una descripción detallada en `/usr/share/doc/packages/sysconfig/README.`

Configuración del sonido

Tras hacer una actualización es necesario volver a configurar las tarjetas de sonido. Esto lo puede hacer con el módulo de sonido de YaST. Como `Root,` escriba `/sbin/yast2 sound`.

Dominio superior `.local` como dominio “enlace-local”

La biblioteca de Resolver trata el dominio superior `.local` como dominio “enlace-local” y envía consultas DNS de multidifusión a la dirección de multidifusión `224.0.0.251,` puerto `5353,` en lugar de enviar consultas DNS normales. Éste es un cambio no compatible. Si el dominio `.local` está siendo ya utilizado en la confi-

guración del servidor de nombres, utilice un nombre de dominio diferente. Para obtener más información sobre el sistema DNS de multidifusión, consulte http://www.multicastdns.org.

Cifrado UTF-8 en todo el sistema

El cifrado por defecto para el sistema es UTF-8. Así pues, al realizar una instalación estándar, se define una configuración regional con cifrado UTF-8, como es_ES.UTF-8. Para obtener más información, consulte http://www.suse.de/~mfabian/suse-cjk/locales.html.

Conversión de nombres de archivos a UTF-8

Los archivos de los sistemas de archivos creados anteriormente no utilizan cifrado UTF-8 para los nombres de archivo (a menos que se especifique lo contrario). Si estos nombres de archivos contienen caracteres no ASCII, aparecerán con caracteres erróneos. Para corregir este problema, utilice el guión convmv, el cual convierte el cifrado de nombres de archivos a UTF-8.

Herramientas de shell compatibles con el estándar POSIX de 2001

En la configuración por defecto, las herramientas de shell del paquete coreutils (tail, chown, head, sort, etc.) ya no cumplen con el estándar POSIX de 1992, pero sí con el de 2001 (*Especificación de UNIX única, versión 3 == IEEE Std 1003.1-2001 == ISO/IEC 9945:2002*). El comportamiento anterior puede forzarse con una variable de entorno:

```
_POSIX2_VERSION=199209
```

El nuevo valor es 200112, y se utiliza como valor por defecto de _POSIX2_VERSION. El estándar SUS puede revisarse (de forma gratuita pero mediante registro) en http://www.unix.org.

SUGERENCIA

Es posible que haya software de otros fabricantes que no cumplan con el nuevo estándar. En este caso, defina la variable de entorno tal y como se ha descrito anteriormente.

Archivo `/etc/gshadow` obsoleto

`/etc/gshadow` se ha eliminado, ya que resulta superfluo por los siguientes motivos:

- No es compatible con glibc.
- No hay interfaz oficial para este archivo. Ni siquiera el paquete duplicado contiene esta interfaz.
- La mayoría de las herramientas que comprueban la contraseña de grupo no son compatibles con el archivo y, por ello, lo ignoran.

OpenLDAP

Dado que el formato de la base de datos ha cambiado, hay que volver a generarlas. Durante el proceso de actualización, el sistema intenta realizar esta conversión automáticamente. No obstante, sin duda habrá casos en los que falle la conversión.

El sistema de comprobación del esquema ha mejorado mucho. Así pues, ya no es posible llevar a cabo varias de las operaciones no compatibles con el estándar que antes era posible realizar con el antiguo servidor LDAP.

La sintaxis del archivo de configuración ha cambiado parcialmente a causa de las listas de control de acceso (ACL). Tras instalar, dispondrá de información sobre la actualización en el archivo `/usr/share/doc/packages/openldap2/README.update`

Sustitución de Apache 1.3 con Apache 2

El servidor Web Apache (versión 1.3) se ha sustituido con Apache 2. En la página Web `http://httpd.apache.org/docs-2.0/en/` hay documentación detallada sobre la versión 2.0. En sistemas con servidores HTTP, las actualizaciones eliminan el paquete de Apache e instalan Apache 2. Después habrá que adaptar el sistema con YaST

o manualmente. Los archivos de configuración de `/etc/httpd` se encuentran ahora en `/etc/apache2.`

Se pueden seleccionar tanto hilos como procesos para gestionar varias consultas concurrentes. La gestión de procesos se ha pasado a un módulo independiente, el módulo de multiprocesamiento (MPM). En consecuencia, Apache 2 necesita el paquete `apache2-prefork` (recomendado por motivos de estabilidad) o el paquete `apache2-worker.` Dependiendo del módulo MPM, Apache 2 reacciona de forma diferente a las consultas. Esto afecta al rendimiento además de al uso de los módulos. Estas características se tratan en detalle en la Sección 26.4.4, “Módulos de multiprocesamiento” (p. 507).

Apache 2 admite ahora la siguiente generación del protocolo de Internet IPv6.

Se ha implementado un mecanismo que permite a los programadores de módulos especificar la secuencia de carga de módulos deseada, tarea que ya no tiene que hacer el usuario. La secuencia en la que se ejecutan los módulos resulta con frecuencia importante. En las versiones anteriores se determinaba a través de la secuencia de carga. De hecho, los módulos que sólo proporcionan acceso a ciertos recursos a usuarios autenticados deberán cargarse primero para evitar que los usuarios sin permiso de acceso puedan ver las páginas.

La consultas a Apache y sus respuestas se pueden procesar mediante filtros.

De Samba 2.x a Samba 3.x

Tras actualizar de Samba 2.x a Samba 3.x no podrá utilizar el sistema de autenticación `winbind.` Todavía se pueden utilizar el resto de métodos de autenticación. Por este motivo se han eliminado los siguientes programas:

```
/usr/sbin/wb_auth
/usr/sbin/wb_ntlmauth
/usr/sbin/wb_info_group.pl
```

Consulte también `http://www.squid-cache.org/Doc/FAQ/FAQ-23.html#ss23.5`.

Actualización de OpenSSH (versión 3.8p1)

La compatibilidad `gssapi` se ha sustituido por `gssapi-with-mic` con objeto de evitar posibles ataques MITM. Estas dos versiones no son compatibles, lo que significa

que no es posible autenticar a partir de distribuciones anteriores de mensajes de Kerberos, ya que se utilizan diferentes métodos de autenticación.

SSH y aplicaciones del terminal

Al establecer una conexión desde un host remoto (especialmente vía SSH, telnet y RSH) entre la versión 9 (configuración estándar con UTF-8 activado) y sistemas más antiguos (SUSE Linux 9.0 y versiones anteriores en las que no está activado UTF-8 por defecto, o no es compatible), las aplicaciones del terminal pueden mostrar caracteres defectuosos.

Esto se debe a que OpenSSH no remite ajustes locales. Así pues, podrían usarse ajustes del sistema por defecto que no coincidieran con los ajustes del terminal remoto. Esto afecta a YaST en modo de texto y a las aplicaciones ejecutadas desde un host remoto como usuario normal (no `Root`). Las aplicaciones iniciadas por parte del usuario `Root` sólo se verán afectadas si el usuario cambia la configuración regional estándar para el `Root` (por defecto sólo se define `LC_CTYPE`).

Eliminación de libiodbc

Los usuarios que utilicen FreeRADIUS ahora deben enlazar a unixODBC, ya que libiodbc ha dejado de funcionar.

Recursos XML en `/usr/share/xml`

Los recursos XML (DTDs, hojas de estilo, etc.) se instalan en `/usr/share/xml`. Así, algunos directorios han dejado de estar disponibles en `/usr/share/sgml`. Si experimenta problemas, modifique los guiones y makefiles o utilice los catálogos oficiales (especialmente `/etc/xml/catalog` o `/etc/sgml/catalog`).

Medios extraíbles con subfs

Los medios extraíbles vienen ahora con subfs integrado. Ya no es necesario montar los medios manualmente con el comando `mount`. Para montar el medio basta con cambiar el directorio del dispositivo correspondiente en `/media`. Los medios no se pueden expulsar si hay algún programa que esté accediendo a ellos.

3.2.2 De la 9.1 a la 9.2

Consulte el artículo “Known Problems and Special Features in SUSE Linux 9.2” (Problemas conocidos y funciones especiales en SUSE Linux 9.2), en la base de datos de asistencia de SUSE en `http://portal.suse.com`, bajo la palabra clave *special features* (funciones especiales).

Activación del cortafuegos en el cuadro de diálogo de propuesta durante la instalación

Para aumentar la seguridad, la solución de cortafuegos adjunta, SuSEFirewall2, se activa al final del proceso de instalación, en el cuadro de diálogo de propuesta. Esto significa que todos los puertos están en un principio cerrados y que, si es necesario, se pueden abrir en el cuadro de diálogo de propuesta. Por defecto, no es posible registrar información desde sistemas remotos. También interfiere con las aplicaciones de multi-difusión y de navegación en la red, como SLP, Samba ("Entorno de red") y algunos juegos. Puede ajustar la configuración del cortafuegos con YaST.

Si es necesario acceder a la red durante la instalación o la configuración de un servicio, el módulo de YaST correspondiente abre los puertos TCP y UDP necesarios de todas las interfaces internas y externas. Si prefiere no hacer uso de esta opción, puede cerrar los puertos en el módulo de YaST o especificar otros ajustes para el cortafuegos.

Compatibilidad entre KDE e IPv6

La compatibilidad con IPv6 no está por defecto habilitada para KDE. Podrá habilitarla mediante el editor de YaST `/etc/sysconfig.` La razón para deshabilitar esta función es que las direcciones IPv6 no son compatibles con todos los proveedores de servicios de Internet y, en consecuencia, se generarían mensajes de error al navegar por la Web y retrasos al mostrar las páginas Web.

Actualización en línea de YaST y paquetes delta

El sistema de actualización en línea de YaST admite ahora una especie de paquete RPM que sólo almacena la diferencia binaria con un paquete base concreto. Esta técnica reduce significativamente el tamaño del paquete y el tiempo de descarga a expensas de una mayor carga de la CPU para volver a montar el paquete final. Indique en `/etc/`

`sysconfig/onlineupdate` si deberá USTED utilizar estos paquetes delta. Consulte `/usr/share/doc/packages/deltarpm/README` para conocer los detalles técnicos.

Configuración del sistema de impresión

Al final de la instalación (cuadro de diálogo de propuesta), los puertos necesarios para el sistema de impresión deben estar abiertos en la configuración del cortafuegos. El puerto 631/TCP y el puerto 631/UDP son necesarios para CUPS y, para que haya un funcionamiento normal, no pueden estar cerrados. El puerto 515/TCP (para el antiguo protocolo LPD) y los puertos que utiliza Samba también deben estar abiertos para imprimir vía LPD o SMB.

Cambio a X.Org

El cambio de XFree86 a X.Org es ahora más fácil gracias a los vínculos de compatibilidad que permiten acceder a archivos y comandos importantes con los nombres antiguos.

Tabla 3.1 *Comandos*

XFree86	X.Org
`XFree86`	`Xorg`
`xf86config`	`xorgconfig`
`xf86cfg`	`xorgcfg`

Tabla 3.2 *Archivos de registro en /var/log*

XFree86	X.Org
`XFree86.0.log`	`Xorg.0.log`
`XFree86.0.log.old`	`Xorg.0.log.old`

Al cambiar a X.Org, el nombre de los paquetes se ha cambiado de `XFree86*` a `xorg-x11*`.

Emuladores de terminal para X11

Se han eliminado una serie de emuladores de terminal, ya que han quedado obsoletos o porque no funcionan en el entorno por defecto, especialmente si no son compatibles con UTF-8. SUSE Linux ofrece terminales estándar, como xterm, los terminales KDE y GNOME y mlterm (emulador de terminal multilingüe para X), que pueden servir como sustitutos de aterm y eterm.

Cambios en el paquete powersave

Los archivos de configuración en `/etc/sysconfig/powersave` han cambiado:

Tabla 3.3 *Archivos de configuración divididos en /etc/sysconfig/powersave*

Antigua	Ahora divididos en
`/etc/sysconfig/powersave/common`	`common`
	`cpufreq`
	`events`
	`battery`
	`sleep`
	`thermal`

`/etc/powersave.conf` ha quedado obsoleto. Las variables existentes han pasado a los archivos que se indican en la Tabla 3.3, “Archivos de configuración divididos en /etc/sysconfig/powersave” (p. 84). Si se han cambiado las variables “event” en `/etc/powersave.conf`, deberán entonces adaptarse en `/etc/sysconfig/powersave/events`.

Los nombres de los estados de sleep han cambiado de:

- Suspender (ACPI S4, suspensión APM)

- Stand-by (ACPI S3, stand-by APM)

A:

- Suspender en disco (ACPI S4, suspensión APM)
- Suspender en RAM (ACPI S3, suspensión APM)
- Stand-by (ACPI S1, stand-by APM)

OpenOffice.org (OOo)

Directorios
: OOo se instala ahora en `/usr/lib/ooo-1.1` en lugar de en `/opt/OpenOffice.org`. El directorio por defecto para los ajustes del usuario es ahora `~/.ooo-1.1` en lugar de `~/OpenOffice.org1.1`.

Empaquetadora
: Ahora hay varias empaquetadoras nuevas para iniciar los componentes de OOo. Puede consultar los nombres nuevos en la Tabla 3.4, "Empaquetadora" (p. 85).

Tabla 3.4 *Empaquetadora*

Antigua	Nuevo
`/usr/X11R6/bin/OOo-calc`	`/usr/bin/oocalc`
`/usr/X11R6/bin/OOo-draw`	`/usr/bin/oodraw`
`/usr/X11R6/bin/OOo-impress`	`/usr/bin/ooimpress`
`/usr/X11R6/bin/OOo-math`	`/usr/bin/oomath`
`/usr/X11R6/bin/OOo-padmin`	`/usr/sbin/oopadmin`
`/usr/X11R6/bin/OOo-setup`	–
`/usr/X11R6/bin/OOo-template`	`/usr/bin/oofromtemplate`
`/usr/X11R6/bin/OOo-web`	`/usr/bin/ooweb`

Antigua	Nuevo
/usr/X11R6/bin/OOo-writer	/usr/bin/oowriter
/usr/X11R6/bin/OOo	/usr/bin/ooffice
/usr/X11R6/bin/OOo-wrapper	/usr/bin/ooo-wrapper

La empaquetadora admite ahora la opción `--icons-set` para cambiar de uno a otro icono de KDE y GNOME. Las opciones que siguen ya no son compatibles: `--default-configuration`, `--gui`, `--java-path`, `--skip-check`, `--lang` (el idioma viene ahora determinado según la configuración regional), `--messages-in-window` y `--quiet`.

Compatibilidad con KDE y GNOME:
Dispone de extensiones de KDE y GNOME en los paquetes `OpenOffice_org-kde` y `OpenOffice_org-gnome`.

Mezclador de sonido kmix

El mezclador de sonido kmix está predefinido por defecto. Para hardware de alta tecnología hay otros mezcladores, como QAMix, KAMix, envy24control (sólo ICE1712) o hdspmixer (sólo RME Hammerfall).

Grabación de DVD

En el pasado, se aplicó un parche al binario `cdrecord` desde el paquete `cdrecord` para que fuera posible grabar discos DVD. Ahora, se instala un nuevo binario `cdrecord-dvd` con este parche.

El programa `growisofs` del paquete `dvd+rw-tools` ahora puede grabar todos los medios DVD (DVD+R, DVD-R, DVD+RW, DVD-RW y DVD+RL). Pruebe a utilizar este paquete en lugar del parche `cdrecord-dvd`.

Varios núcleos

Es posible instalar varios núcleos juntos. Esta función ha sido diseñada para que los administradores puedan actualizar desde un núcleo a otro instalando el nuevo núcleo,

comprobando que funciona como debe y desinstalando después el núcleo antiguo. Mientras que YaST no es aún compatible con esta función, los núcleos se pueden instalar y desinstalar fácilmente desde la shell mediante `rpm -i paquete.rpm`.

Los menús del cargador de arranque por defecto contienen una entrada de núcleo. Antes de instalar varios núcleos, es útil añadir una entrada para los núcleos adicionales, de modo que puedan seleccionarse con facilidad. Puede acceder al núcleo que estaba activo antes de instalar el nuevo núcleo como `vmlinuz.previous` y `initrd.previous`. También se puede acceder al núcleo que estaba activo antes creando una entrada de cargador de arranque similar a la entrada por defecto y haciendo que esta entrada haga referencia a `vmlinuz.previous` y `initrd.previous` en lugar de a `vmlinuz` e `initrd.` GRUB y LILO admiten también entradas de cargador de arranque comodín. Consulte las páginas Info de GRUB (`info grub`) y la página Man `lilo.conf` (5) para obtener información detallada.

3.2.3 De la 9.2 a la 9.3

Consulte el artículo “Known Problems and Special Features in SUSE Linux 9,3” (Problemas conocidos y funciones especiales en SUSE Linux 10), en la base de datos de asistencia de SUSE en `http://portal.suse.com`, bajo la palabra clave *special features* (funciones especiales).

Inicio de la instalación manual en el indicador del núcleo

El modo *Instalación manual* ha desaparecido de la pantalla del cargador de arranque. Todavía puede hacer que linuxrc entre en modo manual con el valor `manual=1` en el indicador de arranque. Normalmente esto no es necesario, ya que puede definir opciones de instalación directamente en el indicador de núcleo, como `textmode=1` o una URL como el origen de instalación.

Kerberos para la autenticación en la red

Para llevar a cabo la autenticación en la red se utiliza `Kerberos,` y no `heimdal.` No es posible convertir una configuración de heimdal existente automáticamente. Durante la actualización del sistema, se crean copias de seguridad de los archivos de

configuración, tal y como se muestra en la Tabla 3.5, “Archivos de copia de seguridad” (p. 88).

Tabla 3.5 *Archivos de copia de seguridad*

Archivo antiguo	Archivo de copia de seguridad
`/etc/krb5.conf`	`/etc/krb5.conf.heimdal`
`/etc/krb5.keytab`	`/etc/krb5.keytab.heimdal`

La configuración del cliente (`/etc/krb5.conf`) es muy parecida a la configuración del cliente en heimdal. Si no se ha configurado nada especial, bastará con sustituir el parámetro `kpasswd_server` por `admin_server`.

No es posible copiar los datos relacionados con el servidor (kdc y kadmind). Tras actualizar el sistema, la base de datos heimdal antigua seguirá disponible en `/var/heimdal`. MIT kerberos mantiene la base de datos en `/var/lib/kerberos/krb5kdc`.

JFS ya no es compatible

Debido a problemas técnicos con JFS, éste ya no es compatible. El controlador del sistema de archivos del núcleo sigue existiendo, si bien YaST no proporciona capacidad de particionamiento con JFS.

AIDE como sustitución de Tripwire

Utilice AIDE (nombre de paquete `aide`), incluido con la licencia GPL, como sistema de detección de intrusiones. Tripwire ya no se incluye en SUSE Linux.

Archivo de configuración de X.Org

La herramienta de configuración SaX2 escribe los ajustes de configuración de X.Org en `/etc/X11/xorg.conf`. Durante una instalación desde cero no se crea ningún enlace de compatibilidad desde `XF86Config` a `xorg.conf`.

Supresión de compatibilidad con XView y OpenLook

Se han suprimido los paquetes `xview`, `xview-devel`, `xview-devel-examples`, `olvwm` y `xtoolpl`. Hasta ahora sólo se proporcionaba el sistema base XView (OpenLook). Tras la actualización del sistema, ya no se incluyen las bibliotecas de XView. Y lo que es más importante, el gestor de ventana virtual de OpenLook, OLVWM, ha dejado de estar disponible.

Configuración de PAM

Nuevos archivos de configuración (con comentarios para mayor información)

`common-auth`
: Configuración de PAM por defecto para la sección auth

`common-account`
: Configuración de PAM por defecto para la sección account

`common-password`
: Configuración de PAM por defecto para cambiar contraseñas

`common-session`
: Configuración de PAM por defecto para gestión de sesiones

Se recomienda incluir estos archivos de configuración por defecto desde dentro del archivo de configuración específico de la aplicación, pues es más fácil modificar y mantener un archivo que los aproximadamente cuarenta archivos que existían en el sistema. Si más adelante instala una aplicación, ésta heredará los cambios aplicados, sin que el administrador tenga que ajustar la configuración.

Los cambios son sencillos. Si tiene el siguiente archivo de configuración (que debería ser el archivo por defecto para la mayoría de las aplicaciones):

```
#%PAM-1.0
auth     required       pam_unix2.so
account  required       pam_unix2.so
password required       pam_pwcheck.so
password required       pam_unix2.so    use_first_pass use_authtok
#password required      pam_make.so     /var/yp
session required        pam_unix2.so
```

puede cambiarlo a:

```
#%PAM-1.0
auth     include        common-auth
account  include        common-account
password include        common-password
session  include        common-session
```

Sintaxis tar más estricta

La sintaxis de uso de `tar` es ahora más estricta. Las opciones de `tar` deben aparecer antes de las especificaciones de archivo o de directorio. Si se añaden opciones como `--atime-preserve` o `--numeric-owner` después de las especificaciones de archivo o de directorio, `tar` fallará. Compruebe sus guiones de copia de seguridad. Comandos como el siguiente han dejado de funcionar:

```
tar czf etc.tar.gz /etc --atime-preserve
```

Consulte las páginas Info de `tar` para obtener más información.

3.2.4 De la 9.3 a la 10.0

Consulte el artículo “Known Problems and Special Features in SUSE Linux 10” (Problemas conocidos y funciones especiales en SUSE Linux 10), en la base de datos de asistencia de SUSE en `http://portal.suse.com`, bajo la palabra clave *special features* (funciones especiales).

Conversión a superusuario con su

Por defecto, al ejecutar `su` para convertirse en usuario `Root` no se define la variable `PATH` para el `Root`. Ejecute `su -` para iniciar una shell de inicio de sesión con el entorno completo para el `Root` o defina `ALWAYS_SET_PATH` en `yes` en `/etc/default/su` si desea cambiar el comportamiento por defecto del comando `su`.

Variables de configuración de ahorro de energía

Los nombres de las variables de configuración de ahorro de energía han cambiado en pro de la coherencia, si bien los archivos sysconfig permanecen igual. Podrá obtener más información en la Sección 33.5.1, “Configuración del paquete powersave” (p. 635).

PCMCIA

`cardmgr` ya no gestiona las tarjetas PC. En lugar de ello, como con las tarjetas CardBus y otros subsistemas, las gestiona un módulo de núcleo. Todas las acciones necesarias se ejecutan con `hotplug`. El guión de inicio `pcmcia` se ha eliminado y `cardctl` se ha sustituido por `pccardctl`. Para obtener más información, consulte `/usr/share/doc/packages/pcmciautils/README.SUSE`.

Configuración de D-BUS para la comunicación entre procesos en .xinitrc

Muchas aplicaciones confían en D-BUS para la comunicación entre procesos (IPC). Al llamar a `dbus-launch` se inicia `dbus-daemon`. El archivo `/etc/X11/xinit/xinitrc` para todo el sistema utiliza `dbus-launch` para iniciar el gestor de ventanas.

Si cuenta con un archivo `~/.xinitrc` local, deberá cambiarlo convenientemente. De lo contrario, aplicaciones como f-spot, banshee, tomboy o Network Manager banshee podrían fallar. Guarde el archivo `~/.xinitrc` antiguo. Copia el nuevo archivo de plantilla en el directorio de inicio con:

```
cp /etc/skel/.xinitrc.template ~/.xinitrc
```

Finalmente, añada sus personalizaciones desde el archivo `.xinitrc` guardado.

Archivos relacionados con NTP renombrados

Por razones de compatibilidad con LSB (Linux Standard Base), a la mayoría de los archivos de configuración y al guión init se les cambió el nombre de `xntp` a `ntp`. Los nuevos nombres de archivo son:

```
/etc/slp.reg.d/ntp.reg

/etc/init.d/ntp

/etc/logrotate.d/ntp

/usr/sbin/rcntp

/etc/sysconfig/ntp
```

Eventos hotplug gestionados por el daemon udev

Los eventos hotplug se gestionan ahora por completo mediante el daemon udev (`udevd`). Ya no se usa el sistema de eventos multiplexor en `/etc/hotplug.d` ni en `/etc/dev.d`. En su lugar, `udevd` llama a las herramientas del ayudante de hotplug directamente según sus reglas. Las reglas de udev y las herramientas del ayudante son proporcionadas por udev y otros paquetes diversos.

Hojas de estilo TEI XSL

Encontrará las hojas de estilo TEI XSL (`tei-xsl-stylesheets`) con una nueva disposición de directorio en `/usr/share/xml/tei/stylesheet/rahtz/current`. Utilice desde aquí, por ejemplo, `base/p4/html/tei.xsl` para generar un resultado HTML. Para obtener más información, consulte `http://www.tei-c.org/Stylesheets/teic/`.

Notificación del cambio del sistema de archivos para aplicaciones GNOME

Para que la funcionalidad sea adecuada, las aplicaciones GNOME dependen de la compatibilidad para la notificación del cambio del sistema de archivos. Para los sistemas de archivos sólo en local, instale el paquete gamin (recomendado) o ejecute el daemon FAM. En el caso de sistemas de archivos remotos, ejecute FAM en el servidor y el cliente y abra el cortafuegos para las llamadas RPC realizadas por FAM.

GNOME (gnome-vfs2 y libgda) contiene una empaquetadora que toma el paquete gamin o fam para ofrecer la notificación del cambio del sistema de archivos:

- Si el daemon FAM no se está ejecutando, se preferirá el paquete gamin (por lo tanto, Inotify es compatible sólo con gamin y es más eficiente para los sistemas de archivos locales).
- Si el daemon FAM se está ejecutanto, se preferirá FAM (por lo tanto: si FAM se está ejecutando, probablemente querrá la notificación remota, que sólo es compatible con FAM).

3.2.5 De la 10.0 a la 10.1

Consulte el artículo “Known Problems and Special Features in SUSE Linux 10” (Problemas conocidos y funciones especiales en SUSE Linux 10), en la base de datos de asistencia de SUSE en `http://portal.suse.com`, bajo la palabra clave *special features* (funciones especiales).

Apache 2.2

En el caso de la versión 2.2 de Apache, el Capítulo 26, *Servidor HTTP Apache* (p. 483) se ha vuelto a redactar por completo. Además, puede encontrar información genérica sobre la actualización en `http://httpd.apache.org/docs/2.2/upgrading.html` y una descripción de las nuevas funciones en `http://httpd.apache.org/docs/2.2/new_features_2_2.html`.

Inicio de servidores FTP (vsftpd)

Por defecto, `xinetd` ya no inicia el servidor FTP `vsftpd`. Ahora es un daemon autónomo y debe configurarlo con el editor del tiempo de ejecución de YaST.

Firefox 1.5: comando de apertura de URL

Con Firefox 1.5, el método de las aplicaciones para abrir una instancia o ventana de Firefow ha cambiado. El nuevo método ya estaba parcialmente disponible en versiones anteriores en las que se implementó el comportamiento en el guión de la empaquetadora.

Si la aplicación no utiliza `mozilla-xremote-client` ni `firefox -remote`, no tendrá que cambiar nada. De lo contrario, el nuevo comando que abra una URL será `firefox` *`url`* y no importará si Firefox ya se está ejecutando o no. Si ya se está ejecutanto, seguirá la preferencia configurada en la opción para abrir enlaces de otras aplicaciones.

En la línea de comandos, puede influir en el comportamiento usando `firefox -new-window` *`url`* o `firefox -new-tab` *`url`*.

3.3 Gestor de paquetes RPM

En SUSE Linux, el RPM (gestor de paquetes RPM) se utiliza para gestionar los paquetes de software. Los programas principales que lo componen son `rpm` y `rpmbuild`. Los usuarios, los administradores del sistema y los creadores de paquetes pueden realizar consultas a la potente base de datos RPM para obtener información detallada acerca del software instalado.

Básicamente, `rpm` dispone de cinco modos: instalación, desinstalación y actualización de los paquetes de software; reconstrucción de la base de datos RPM; consulta a las bases de RPM o los archivos de reserva RPM individuales; comprobación de la integridad de los paquetes y, por último, la firma de los paquetes. El comando `rpmbuild` puede utilizarse para generar paquetes instalables a partir de orígenes antiguos.

Los archivos de reserva RPM instalables están empaquetados con un formato binario especial. Estos archivos constan de archivos de programa para su instalación y metainformación que `rpm` utilizará durante la instalación para configurar el paquete de software o que se almacenará en la base de datos RPM para que sirva de documentación. Los archivos de reserva RPM normalmente tienen la extensión `.rpm`.

SUGERENCIA: Paquetes de desarrollo de software

En un buen número de paquetes, los componentes necesarios para el desarrollo del software (bibliotecas, encabezados, archivos include, etc.) se han colocado en paquetes independientes. Estos paquetes de desarrollo sólo son necesarios si desea compilar el software usted mismo, como en el caso de los paquetes GNOME más recientes. Se pueden identificar mediante la extensión del nombre `-devel` como, por ejemplo, paquetes `alsa-devel, gimp-devel` y `kdelibs3-devel`.

3.3.1 Comprobación de la autenticidad de los paquetes

Los paquetes RPM de SUSE Linux cuentan con una firma GnuPG. La clave incluida la huella digital es:

```
1024D/9C800ACA 2000-10-19 SuSE Package Signing Key <build@suse.de>
Key fingerprint = 79C1 79B2 E1C8 20C1 890F  9994 A84E DAE8 9C80 0ACA
```

El comando `rpm --checksig` *`paquete`*`-1.2.3.rpm` puede utilizarse para comprobar la firma de un paquete RPM a fin de determinar si realmente tiene su origen en SUSE Linux o en otro sistema de confianza. El uso de este comando es muy recomendable para actualizar paquetes desde Internet. La clave pública de la firma del paquete de SUSE Linux reside normalmente en `/root/.gnupg/`. La clave se encuentra ubicada también en el directorio `/usr/lib/rpm/gnupg/`, para permitir que los usuarios normales comprueben la firma de los paquetes RPM.

3.3.2 Gestión de paquetes: instalación, actualización y desinstalación

Normalmente, la instalación de un archivo de reserva RPM es bastante sencilla: `rpm -i` *`paquete`*`.rpm`. Con este comando se instala el paquete, pero sólo si se cumplen las dependencias y no hay conflictos con otros paquetes. Mediante un mensaje de error, `rpm` pide los paquetes que tienen que instalarse para cumplir con los requisitos de dependencias. En segundo plano, la base de datos RPM se asegura de que no surjan conflictos (un archivo concreto sólo puede pertenecer a un paquete). Al seleccionar diferentes opciones, puede forzar a `rpm` a hacer caso omiso de estos valores por defecto. Sin embargo, hay que ser un usuario experto para utilizarlas. De lo contrario, existe el riesgo de afectar a la integridad del sistema y poner en peligro la capacidad de actualización del sistema.

Las opciones `-U` o `--upgrade` y `-F` o `--freshen` pueden utilizarse para actualizar un paquete; por ejemplo, `rpm -F` *`paquete`*`.rpm`. Este comando desinstala los archivos de la versión anterior e instala los nuevos inmediatamente. La diferencia entre las dos versiones estriba en que `-U` instala paquetes que no existían previamente en el sistema mientras que `-F` sólo actualiza paquetes previamente instalados. Al actualizar, `rpm` actualiza los archivos de configuración con cuidado usando la siguiente estrategia:

- Si el administrador del sistema no ha cambiado un archivo de configuración, `rpm` instalará la nueva versión del archivo adecuado. No es necesario que el administrador del sistema realice ninguna acción.

- Si el administrador del sistema ha cambiado un archivo de configuración antes de la actualización, `rpm` guarda el archivo modificado con la extensión `.rpmorig` o `.rpmsave` (archivo de copia de seguridad) e instala la versión del nuevo paquete,

siempre y cuando el archivo instalado en un principio y la versión más reciente sean diferentes. Si es así, compare el archivo de copia de seguridad (`.rpmorig` o `.rpmsave`) con el archivo recién instalado y realice los cambios otra vez en el archivo nuevo. Después, asegúrese de suprimir todos los archivos `.rpmorig` y `.rpmsave` para evitar problemas con futuras actualizaciones.

- Los archivos `.rpmnew` aparecen si el archivo de configuración ya existe *y* si la etiqueta `noreplace` está especificada en el archivo `.spec`.

Después de la actualización, se deben eliminar los archivos `.rpmsave` y `.rpmnew` después de compararlos, de manera que no obstaculicen futuras actualizaciones. La extensión `.rpmorig` se asigna si la base de datos RPM no ha reconocido previamente el archivo.

De lo contrario, se usará `.rpmsave.` En otras palabras, `.rpmorig` es el resultado de actualizar a partir de un formato ajeno a RPM. `.rpmsave` es el resultado de actualizar a partir de un RPM antiguo a uno más reciente. `.rpmnew` no revela ninguna información, como que el administrador del sistema haya realizado cambios en el archivo de configuración. Hay disponible una lista de estos archivos en `/var/adm/rpmconfigcheck.` Algunos archivos de configuración (como `/etc/httpd/httpd.conf`) no se sobrescriben para que no haya interrupciones en las operaciones.

El parámetro `-U` *no* es sólo el equivalente para desinstalar con la opción `-e` e instalar con la opción `-i`. Utilice `-U` cuando sea posible.

Para desinstalar un paquete, escriba `rpm -e` *`paquete`*. El comando `rpm` sólo suprimirá el paquete si no hay dependencias sin resolver. Teóricamente es imposible suprimir Tcl/Tk, por ejemplo, mientras otra aplicación lo necesite. Incluso en este caso, RPM pide ayuda desde la base de datos. Si tal supresión es, por las razones que sean y en circunstancias poco usuales, imposible aun en el caso de que *no* existan dependencias adicionales, puede resultar de ayuda volver a generar la base de datos RPM mediante la opción `--rebuilddb`.

3.3.3 RPM y revisiones

Para garantizar la seguridad operativa de un sistema, se deben instalar en el sistema los paquetes de actualización de vez en cuando. Antes, un error en un paquete sólo podía solucionarse sustituyendo todo el paquete. Los paquetes grandes con errores en archivos

de pequeño tamaño podían dar como resultado grandes cantidades de datos. Sin embargo, SUSE RPM ofrece una función que permite la instalación de revisiones en paquetes.

Los aspectos más importantes se explican usando "pine" como ejemplo:

¿Es el RPM de revisión adecuado para mi sistema?
: Para comprobarlo, realice una consulta sobre la versión instalada del paquete. Para pine, esto puede realizarse de esta forma:

```
rpm -q pino
pino-4.44-188
```

Compruebe a continuación si el RPM de revisión es adecuado para esta versión de pine:

```
rpm -qp --basedon pine-4.44-224.i586.patch.rpm
pine = 4.44-188
pine = 4.44-195
pine = 4.44-207
```

Esta revisión es adecuada para tres versiones diferentes de pine. La versión instalada en el ejemplo también se muestra de manera que la revisión pueda instalarse.

¿Qué archivos sustituye la revisión?
: Los archivos afectados por una revisión pueden verse fácilmente en el RPM de revisión. El parámetro `rpm -P` permite la selección de funciones de revisión especiales. Muestre la lista de archivos con el comando siguiente:

```
rpm -qpPl pine-4.44-224.i586.patch.rpm
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

O bien, si la revisión ya se ha instalado, con el comando siguiente:

```
rpm -qPl pine
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

¿Cómo puede un RPM de revisión instalarse en el sistema?
: Los RPM de revisión se usan como RPM normales. La única diferencia es que un RPM adecuado debe estar ya instalado.

¿Qué revisiones están ya instaladas en el sistema y para qué versiones del paquete?
Se puede mostrar una lista de todas las revisiones instaladas en el sistema con el comando `rpm -qPa`. Si sólo se ha instalado una revisión en un sistema nuevo (como en este ejemplo), la lista aparecerá de la siguiente manera:

```
rpm -qPa
pine-4.44-224
```

Si, posteriormente, desea saber la versión del paquete instalada en un primer momento, esta información también estará disponible en la base de datos RPM. Para `pine`, esta información puede mostrarse con el siguiente comando:

```
rpm -q --basedon pine
pine = 4.44-188
```

Hay más información, incluso sobre la función de revisión de RPM, disponible en las páginas Man de `rpm` y `rpmbuild`.

3.3.4 Paquetes RPM delta

Los paquetes RPM delta contienen las diferencias entre una versión antigua y una nueva de un paquete RPM. Aplicar un RPM delta en un RPM antiguo da como resultado un RPM completamente nuevo. No es necesario contar con una copia de un RPM antiguo porque un RPM delta también puede funcionar con un RPM instalado. Los paquetes RPM delta tienen incluso un tamaño más pequeño que los RPM de revisión, lo que supone una ventana a la hora de transferir los paquetes de actualización por Internet. El inconveniente radica en que las actualizaciones con los RPM delta consumen muchos más ciclos de CPU que los RPM de revisión o los normales. Para que YaST utilice los paquetes RPM delta durante las sesiones de YOU, defina `YOU_USE_DELTAS` en `yes` (sí) en `/etc/sysconfig/onlineupdate`. En este caso, tenga preparados los medios de instalación. Si `YOU_USE_DELTAS` está vacío o definido en `filesystem`, YOU intentará descargar los paquetes delta que se aplicarán a los archivos instalados. En este caso no serán necesarios los medios de instalación, pero el tiempo de descarga podría ser mayor. Si está definido en `no`, YOU sólo usará RPM de revisión y normales.

Los binarios `prepdeltarpm`, `writedeltarpm` y `applydeltarpm` forman parte del paquete RPM delta (paquete `deltarpm`), y ayudan a crear y a aplicar paquetes RPM delta. Con los comandos siguientes, cree un RPM delta denominado `nuevo.delta.rpm`. El siguiente comando asume que `antiguo.rpm` y `nuevo.rpm` están presentes:

```
prepdeltarpm -s seq -i info antiguo.rpm > old.cpio
prepdeltarpm -f nuevo.rpm > nuevo.cpio

xdelta delta -0 old.cpio nuevo.cpio delta

writedeltarpm nuevo.rpm delta info nuevo.delta.rpm
rm antiguo.cpio nuevo.cpio delta
```

Con `applydeltarpm` podrá reconstruir el RPM nuevo desde el sistema de archivos si el paquete antiguo ya está instalado:

```
applydeltarpm nuevo.delta.rpm nuevo.rpm
```

Para derivarlo desde el RPM antiguo sin tener que acceder al sistema de archivos, utilice la opción `-r`:

```
applydeltarpm -r antiguo.rpm nuevo.delta.rpm nuevo.rpm
```

Consulte `/usr/share/doc/packages/deltarpm/README` para conocer los detalles técnicos.

3.3.5 Consultas de RPM

Con la opción `-q`, `rpm` inicia las consultas, posibilitando la inspección de un archivo de reserva RPM (añadiendo la opción `-p`) y además realizando consultas a la base de datos RPM de los paquetes instalados. Hay varios parámetros disponibles para especificar el tipo de información necesaria. Consulte la Tabla 3.6, “Opciones de consulta más importantes de RPM” (p. 99).

Tabla 3.6 *Opciones de consulta más importantes de RPM*

`-i`	Información del paquete
`-l`	Lista de archivos
`-f` `NOMBREARCHIVO`	Realiza una consulta al paquete que contiene el archivo *`NOMBREARCHIVO`* (la vía completa debe especificarse en *`NOMBREARCHIVO`*)
`-s`	Lista de archivos con información de estado (implica `-l`)

`-d`	Lista con los archivos de documentación solamente (implica `-l`)
`-c`	Lista con los archivos de configuración solamente (implica `-l`)
`--dump`	Lista de archivos con información completa (para su uso con `-l`, `-c` o `-d`)
`--provides`	Lista de funciones del paquete que otro paquete puede solicitar con `--requires`
`--requires`, `-R`	Capacidades que necesita el paquete
`--scripts`	Guiones de instalación (instalación previa, posterior y desinstalación)

Por ejemplo, el comando `rpm -q -i wget` muestra la información mostrada en el Ejemplo 3.2, “rpm -q -i wget” (p. 100).

Ejemplo 3.2 *rpm -q -i wget*

```
Name        : wget                         Relocations: (not relocatable)
Version     : 1.9.1                             Vendor: SUSE LINUX AG,
Nuernberg, Germany
Release     : 50                            Build Date: Sat 02 Oct 2004
03:49:13 AM CEST
Install date: Mon 11 Oct 2004 10:24:56 AM CEST      Build Host: f53.suse.de
Group       : Productivity/Networking/Web/Utilities   Source RPM:
wget-1.9.1-50.src.rpm
Size        : 1637514                          License: GPL
Signature   : DSA/SHA1, Sat 02 Oct 2004 03:59:56 AM CEST, Key ID
a84edae89c800aca
Packager    : http://www.suse.de/feedback
URL         : http://wget.sunsite.dk/
Summary     : A tool for mirroring FTP and HTTP servers
Description :
Wget enables you to retrieve WWW documents or FTP files from a server.
This can be done in script files or via the command line.
[...]
```

La opción `-f` sólo funciona si especifica el nombre de archivo completo con su vía. Escriba tantos nombres de archivo como desee. Por ejemplo, el siguiente comando:

```
rpm -q -f /bin/rpm /usr/bin/wget
```

da como resultado:

```
rpm-4.1.1-191
wget-1.9.1-50
```

Si sólo se sabe una parte del nombre del archivo, utilice un guión de shell tal y como se muestra en el Ejemplo 3.3, “Guión para buscar paquetes” (p. 101). Pase el nombre parcial del archivo al guión como un parámetro cuando lo ejecute.

Ejemplo 3.3 *Guión para buscar paquetes*

```
#! /bin/sh
for i in $(rpm -q -a -l | grep  $1); do
    echo "\"$i\" is in package:"
    rpm -q -f $i
    echo ""
done
```

El comando `rpm -q --changelog rpm` muestra una lista detallada de información de cambios sobre un paquete específico ordenados por fecha. Este ejemplo muestra información sobre el paquete `rpm`.

Con la ayuda de la base de datos RPM instalada, se pueden realizar comprobaciones de verificación. Inícielas con `-V`, `-y` o `--verify`. Con esta opción, `rpm` muestra todos los archivos de un paquete que han cambiado desde la instalación. `rpm` utiliza símbolos de ocho caracteres para proporcionar algunas sugerencias sobre los cambios siguientes:

Tabla 3.7 *Opciones de verificación de RPM*

`5`	Suma de comprobación MD5
`S`	Tamaño de archivo
`L`	Enlace simbólico
`T`	Hora de modificación
`D`	Números de dispositivos principales y secundarios
`U`	Propietario
`G`	Group

En el caso de los archivos de configuración, se imprime la letra `c`. Por ejemplo, para cambios a `/etc/wgetrc` (`wget`):

```
rpm -V wget
S.5....T c /etc/wgetrc
```

Los archivos de la base de datos RPM se colocan en `/var/lib/rpm`. Si la partición `/usr` tiene un tamaño de 1 GB, esta base de datos puede ocupar casi 30 MB, sobre todo después de una actualización completa. Si la base de datos es mucho más grande de lo esperado, resulta muy útil reconstruirla con la opción `--rebuilddb`. Antes de hacerlo, realice una copia de seguridad de la base de datos antigua. El guión `cron cron.daily` realiza copias diarias de la base de datos (empaquetadas con gzip) y las almacena en `/var/adm/backup/rpmdb`. El número de copias está controlado mediante la variable `MAX_RPMDB_BACKUPS` (por defecto: `5`) en `/etc/sysconfig/backup`. El tamaño de una copia de seguridad es de aproximadamente 1 MB para 1 GB en `/usr`.

3.3.6 Instalación y compilación de los paquetes fuente

Todos los paquetes fuente de SUSE Linux llevan la extensión `.src.rpm` (RPM fuente).

SUGERENCIA

Los paquetes fuente pueden copiarse desde el medio de instalación en el disco duro y desempaquetarse con YaST. Sin embargo, en el gestor de paquetes no aparecen marcados como instalados (`[i]`). Esto se debe a que los paquetes fuente no se introducen en la base de datos RPM. Sólo aparece en ella el software del sistema operativo *instalado*. Cuando "instala" un paquete fuente, sólo se añadirá el código fuente al sistema.

Los siguientes directorios deben estar disponibles para `rpm` y `rpmbuild` en `/usr/src/packages` (a menos que haya especificado los ajustes personalizados en un archivo como `/etc/rpmrc`):

SOURCES
: Es el directorio para las fuentes originales (archivos `.tar.bz2` o `.tar.gz`, etc.) y para los ajustes específicos de distribución (sobre todo para archivos `.diff` o `.patch`).

SPECS
: Es el directorio para archivos *.spec,* similares a meta makefiles, que controlan el proceso de *construcción.*

BUILD
: Todos las fuentes se desempaquetan, se revisan y compilan en este directorio.

RPMS
: Lugar donde se almacenan los paquetes binarios finalizados.

SRPMS
: Aquí se encuentran los RPM fuente.

Cuando instala un paquete fuente con YaST, todos los componentes necesarios se instalan en `/usr/src/packages`: las fuentes y los ajustes en SOURCES y el archivo `.spec` relevante en SPECS.

AVISO

No haga experimentos con los componentes del sistema (`glibc`, `rpm`, `sysvinit`, etc.) ya que pondría en peligro el funcionamiento del sistema.

En el siguiente ejemplo se utiliza el paquete `wget.src.rpm`. Después de instalar el paquete con YaST, debería tener archivos similares a la siguiente lista:

```
/usr/src/packages/SOURCES/nops_doc.diff
/usr/src/packages/SOURCES/toplev_destdir.diff
/usr/src/packages/SOURCES/wget-1.9.1+ipvmisc.patch
/usr/src/packages/SOURCES/wget-1.9.1-brokentime.patch
/usr/src/packages/SOURCES/wget-1.9.1-passive_ftp.diff
/usr/src/packages/SOURCES/wget-LFS-20040909.tar.bz2
/usr/src/packages/SOURCES/wget-wrong_charset.patch
/usr/src/packages/SPECS/wget.spec
```

`rpmbuild -b` *`X`* `/usr/src/packages/SPECS/wget.spec` inicia la compilación. *X* es un comodín para varias fases del proceso de construcción (consulte la salida de `--help` o la documentación de RPM para obtener más información). A continuación sólo se ofrece una breve explicación:

`-bp`
: Prepara las fuentes en `/usr/src/packages/BUILD:` desempaqueta y revisa.

`-bc`
: Hace lo mismo que `-bp` pero realiza una compilación adicional.

`-bi`
: Hace lo mismo que `-bp` pero instala además el software creado. Precaución: si el paquete no admite la función BuildRoot, podría sobrescribir los archivos de configuración.

`-bb`
: Hace lo mismo que `-bi` pero crea además el paquete binario. Si la compilación se ha realizado correctamente, el archivo binario debería estar en `/usr/src/packages/RPMS.`

`-ba`
: Hace lo mismo que `-bb` pero crea además el RPM fuente. Si la compilación se ha realizado correctamente, el archivo binario debería estar en `/usr/src/packages/SRPMS.`

`--short-circuit`
: Omite algunos pasos.

El RPM binario creado pueda instalarse ahora con `rpm -i` o preferiblemente con `rpm -U`. La instalación con `rpm` hace que aparezca en la base de datos RPM.

3.3.7 Compilación de los paquetes RPM con build

El peligro de manejar muchos paquetes es que se añaden archivos no deseados al sistema que se está ejecutando durante el proceso de creación. Para evitarlo, use el guión `build`, que crea un entorno definido en el que se crea el paquete. Para establecer este entorno chroot, el guión `build` debe contar con un árbol de paquetes completo. Este árbol puede estar disponible en el disco duro, mediante NFS o desde el DVD. Defina la posición con `build --rpms` *`directorio`*. A diferencia de `rpm`, el comando `build` busca el archivo SPEC en el directorio de origen. Para crear wget (como en el ejemplo anterior) con el DVD montado en el sistema en `/media/dvd,` utilice los siguientes comandos como `usuario Root:`

```
cd /usr/src/packages/SOURCES/
mv ../SPECS/wget.spec .
build --rpms /media/dvd/suse/ wget.spec
```

Posteriormente se establecerá un entorno mínimo en `/var/tmp/build-root`. El paquete se creará en este entorno. Al terminar, los paquetes resultantes estarán situados en `/var/tmp/build-root/usr/src/packages/RPMS`.

El guión `build` ofrece algunas opciones adicionales. Por ejemplo, provoca que el guión prefiera sus propios RPM, omite la inicialización del entorno de creación o limita el comando `rpm` a una de las fases anteriormente mencionadas. Acceda a información adicional mediante `build --help` o leyendo la página Man de `build`.

3.3.8 Herramientas para los archivos de reserva RPM y la base de datos RPM

Midnight Commander (`mc`) puede mostrar los contenidos de los archivos de reserva RPM y copiar algunas partes. Representa archivos de reserva como sistemas de archivos virtuales, ofreciendo todas las opciones de menú usuales de Midnight Commander. Muestre el archivo HEADER con F3. Eche un vistazo a la estructura de los archivos de reserva con las teclas de cursor e Intro. Copie los componentes de los archivos de reserva con F5.

KDE ofrece la herramienta kpackage como interfaz de usuario para `rpm`. Hay disponible un gestor de paquetes con funcionalidad completa como módulo de YaST (consulte la Sección “Instalación y desinstalación del software” (Capítulo 2, *Configuración del sistema con YaST*, ↑Inicio)).

Parte 2. Administración

4 Seguridad en Linux

La función de enmascaramiento y el cortafuegos garantizan el control en el flujo y el intercambio de los datos. SSH (shell seguro) permite iniciar la sesión en hosts remotos a través de una conexión cifrada. El cifrado de archivos o de particiones completas protege los datos en el caso de que usuarios externos consigan acceder al sistema. Además de instrucciones técnicas, se incluye información acerca de los aspectos relacionados con la seguridad de las redes Linux.

4.1 Enmascaramiento y cortafuegos

Siempre que Linux se utiliza en un entorno de red, se pueden emplear las funciones del núcleo que permiten la manipulación de los paquetes de red para conservar una separación entre las áreas de redes interna y externa. La estructura de Linux netfilter proporciona los recursos para instalar un cortafuegos efectivo que gestione las diferentes redes de forma distinta. Con la ayuda de iptables —una estructura genérica de tabla para la definición de los conjuntos de tablas—, controle de forma exhaustiva los paquetes que se permite que pasen a una interfaz de red. Este filtro de paquetes se puede configurar de forma relativamente sencilla con la ayuda de SuSEfirewall2 y el módulo YaST correspondiente.

4.1.1 Filtrado de paquetes con iptables

Los elementos netfilter e iptables son responsables del filtrado y de la manipulación de paquetes de redes, así como de la NAT (conversión de direcciones de red). Los criterios de filtrado y cualquier acción relacionada con ellos se almacenan en cadenas, que se

agrupan una tras otra por paquetes de red individuales cada vez que se reciben. Las cadenas que se deben ordenar se almacenan en tablas. El comando `iptables` le permite alterar estas tablas y los conjuntos de reglas.

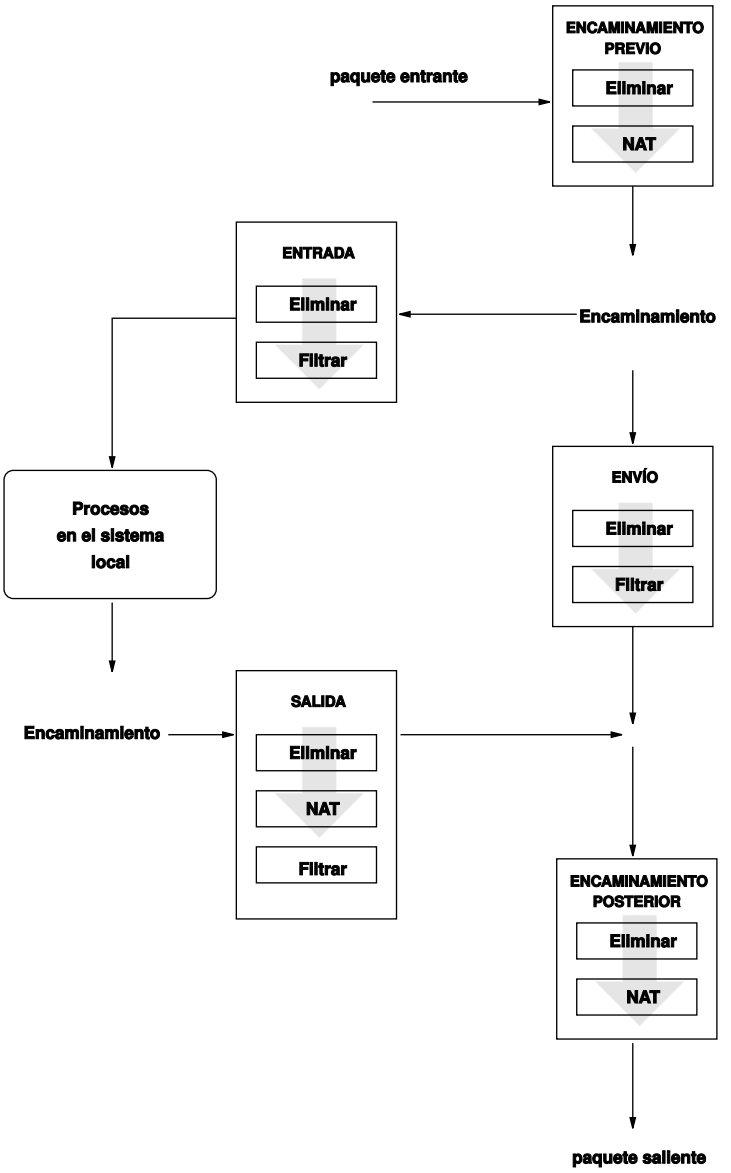
El núcleo de Linux mantiene tres tablas, cada una de ellas destinada a una categoría determinada de funciones del filtro de paquetes:

filter
: Esta tabla incluye la totalidad de las reglas de filtros, debido a que implementa el mecanismo *filtrado de paquetes* en sentido estricto, lo que determina, por ejemplo, si se permiten los paquetes (`ACCEPT`) o si se descartan (`DROP`).

nat
: Esta tabla define todos los cambios realizados en las direcciones de origen y destino de los paquetes. Haciendo uso de estas funciones podrá también recurrir al *enmascaramiento*, que es un caso especial de NAT que se emplea para enlazar una red privada a Internet.

mangle
: Las reglas contenidas en esta tabla permiten manipular los valores almacenados en los encabezados IP (como, por ejemplo, el tipo de servicio).

Figura 4.1 *iptables: posibles vías del paquete*



Estas tablas contienen varias cadenas predefinidas para la coincidencia de paquetes:

ENCAMINAMIENTO PREVIO
: Esta cadena se aplica a los paquetes entrantes.

ENTRADA
: Esta cadena se aplica a los paquetes destinados a los procesos internos del sistema.

ENVÍO
: Esta cadena se aplica solamente a los paquetes que se enrutan a través del sistema.

SALIDA
: Esta cadena se aplica a los paquetes originados en el sistema.

ENCAMINAMIENTO POSTERIOR
: Esta cadena se aplica a todos los paquetes salientes.

La Figura 4.1, “iptables: posibles vías del paquete” (p. 111) ilustra las vías por las que puede desplazarse un paquete de red en un sistema dado. Por razones de simplicidad, las ilustración muestra las tablas como partes de las cadenas, pero en realidad estas cadenas se sustentan en las propias tablas.

La más sencilla de las situaciones se produce cuando un paquete de entrada destinado al sistema llega a la interfaz `eth0`. En primer lugar, el paquete se deriva a la cadena `PREROUTING` de la tabla `mangle` y, a continuación, a la cadena `PREROUTING` de la tabla `nat`. El siguiente paso, referido al enrutamiento del paquete, establece que el destino real del paquete es un proceso del sistema. Después de pasar por las cadenas `INPUT` de las tablas `mangle` y `filter`, el paquete alcanza finalmente su objetivo, debido a que las reglas de la tabla `filter` son coincidentes.

4.1.2 Nociones básicas sobre el enmascaramiento

El enmascaramiento es la forma específica de NAT (conversión de direcciones de red) de Linux Se puede emplear para conectar una LAN pequeña (donde los hosts utilizan direcciones IP de rango privado; a este respecto, consulte la Sección 18.1.2, “Máscaras de red y encaminamiento” (p. 349)) a Internet (donde se emplean direcciones IP oficiales). Para que los hosts de la LAN puedan conectarse a Internet, sus direcciones privadas se traducen en direcciones oficiales. Esta operación se realiza en el router, que actúa de gateway entre la LAN e Internet. El principio subyacente es muy sencillo: El router tiene más de una interfaz de red, normalmente una tarjeta de red y una interfaz que lo

conecta a Internet. Mientras que esta última enlaza el router con el exterior, una o varias de las demás lo conectan a los hosts de LAN. Con los hosts de la red local conectados a la tarjeta de red (como por ejemplo `eth0`) del router, es posible enviar cualquier paquete no destinado a la red local a su gateway o router por defecto.

IMPORTANTE: Utilización de la máscara de red adecuada

Cuando configure su red, asegúrese de que tanto la dirección de difusión como la máscara de red son las mismas para todos los hosts locales. Si no toma esta precaución, los paquetes no se enrutarán adecuadamente.

Como se ha mencionado, cuando uno de los hosts de LAN envía un paquete destinado a una dirección de Internet, éste se dirige al router por defecto. Sin embargo, el router debe configurarse antes de poder reenviar los paquetes. Por razones de seguridad, SUSE Linux no habilita esta función en una instalación por defecto. Para habilitarla, fije la variable `IP_FORWARD` en el archivo `/etc/sysconfig/sysctl` como `IP_FORWARD=yes`.

El host de destino de la conexión puede tener constancia de la existencia de su router, pero no dispone de información acerca del host que se encuentra situado en la red interna y que es donde se originaron los paquetes. Por esta razón esta técnica se denomina enmascaramiento. A consecuencia de la conversión de direcciones, el router es el primer destino de todos los paquetes de respuesta. El router debe identificar estos paquetes entrantes y traducir sus direcciones de destino, de forma tal que los paquetes se reenvíen al host adecuado de la red local.

Gracias al enrutamiento del tráfico entrante dependiente de la tabla de enmascaramiento, no existe ninguna manera de abrir una conexión con un host interno desde el exterior. Para una conexión de este tipo no habría ninguna entrada en la tabla. Además, a cada conexión que se encuentre establecida se le asigna una entrada de estado en la tabla, por lo que la entrada no podrá emplear ninguna otra conexión.

Como consecuencia, es posible que se produzcan problemas con un número determinado de protocolos de aplicación, tales como ICQ, cucme, IRC (DCC, CTCP) y FTP (en modo PORT). Netscape, el programa FTP y muchos otros programas utilizan el modo PASV. Este modo pasivo origina muchos menos problemas en lo referente al enmascaramiento y filtrado de paquetes.

4.1.3 Nociones básicas sobre el empleo de cortafuegos

El término *cortafuegos* es probablemente el que se emplea con mayor frecuencia para describir un mecanismo que proporciona y gestiona un enlace entre redes al tiempo que controla también el flujo de datos entre ellos. Estrictamente hablando, el mecanismo que se describe en esta sección se denomina *filtro de paquetes*. El filtro de paquetes regula el flujo de datos de acuerdo con determinados criterios, tales como protocolos, puertos y direcciones IP. De esta manera, es posible bloquear paquetes que, de acuerdo con sus direcciones de origen, se pretende que no lleguen a su red. Para permitir el acceso público a, por ejemplo, su servidor Web, abra de forma explícita el puerto correspondiente. Sin embargo, el filtro de paquetes no examina el contenido de los paquetes provenientes de direcciones legítimas, como por ejemplo aquéllos que se envían a su servidor Web. Por ejemplo, si los paquetes entrantes están dirigidos a modificar un programa CGI de su servidor Web, el filtro de paquetes permitirá su acceso.

Un mecanismo más efectivo pero también más complejo es la combinación de distintos tipos de sistemas, como por ejemplo la interacción de un filtro de paquetes con un gateway o alterno de aplicación. En este caso, el filtro de paquetes rechaza cualquier paquete que tenga como objetivo la inhabilitación de puertos. Únicamente se aceptan los paquetes dirigidos a la gateway de aplicación. Esta gateway o este alterno simula ser el cliente real del servidor. En cierto modo, dicho alterno puede considerarse un host de enmascaramiento en el nivel de protocolo empleado por la aplicación. Un ejemplo para un alterno de este tipo es Squid, un servidor alterno HTTP. Para utilizar Squid, el navegador se debe configurar para que se pueda comunicar a través del alterno. Cualquier página HTTP que se solicite se sirve a partir de la caché alterna; en cuanto a las páginas no encontradas en la caché, éstas las recupera el alterno de Internet. En otro orden de cosas, el paquete SUSE Proxy-Suite (`proxy-suite`) proporciona un alterno para el protocolo.

La siguiente sección se centra en el filtro de paquetes que se proporciona con SUSE Linux. Para obtener más información sobre el filtrado de paquetes y el empleo de cortafuegos, consulte el documento Firewall HOWTO, que se incluye en el paquete `howto`. Si este paquete se encuentra ya instalado, lea el documento HOWTO mediante la opción `less /usr/share/doc/howto/en/txt/Firewall-HOWTO.gz`.

4.1.4 SuSEfirewall2

SuSEfirewall2 es un guión que lee las variables establecidas en `/etc/sysconfig/SuSEfirewall2` para generar un juego de reglas de iptables. Se definen tres zonas de seguridad, aunque solamente se consideran la primera y la segunda en el siguiente ejemplo de configuración:

Zona externa
: Debido a que no existe ninguna manera de controlar lo que sucede en la red externa, el host necesita estar protegido de dicha red. En la mayoría de los casos, la red externa es Internet, pero también podría tratarse de otra red insegura, como por ejemplo una red WLAN.

Zona interna
: Hace referencia a la red privada, en la mayoría de los casos una red LAN. Si los hosts de esta red utilizan direcciones IP de rango privado (a este respecto, consulte la Sección 18.1.2, “Máscaras de red y encaminamiento” (p. 349)), habilite la conversión de direcciones de red (NAT), de forma tal que los hosts de la red interna puedan acceder a la red externa.

Zona desmilitarizada (DMZ)
: Mientras que se puede llegar a los hosts que se ubican en esta zona tanto desde la red externa como interna, dichos hosts no pueden acceder a la red interna. Esta configuración puede emplearse para incluir una línea adicional de defensa ante la red interna, debido a que los sistemas DMZ están aislados de la red interna.

Todo tipo de tráfico de red no permitido de forma expresa por la regla de filtrado se suprime por la acción de las iptables. Por lo tanto, cada una de las interfaces con tráfico de entrada deben ubicarse en una de las tres zonas. Defina los servicios o protocolos permitidos para cada una de las zonas. La regla que se establezca se aplica solamente a los paquetes procedentes de hosts remotos. Los paquetes generados en la zona local no son capturados por el cortafuegos.

La configuración se puede realizar con YaST (a este respecto, consulte “Configuración con YaST” (p. 116)). También se puede llevar a cabo de forma manual en el archivo `/etc/sysconfig/SuSEfirewall2`, que se encuentra convenientemente comentado. En otro orden de cosas, se encuentra disponible a modo de ejemplo una serie de situaciones en `/usr/share/doc/packages/SuSEfirewall2/EXAMPLES`.

Configuración con YaST

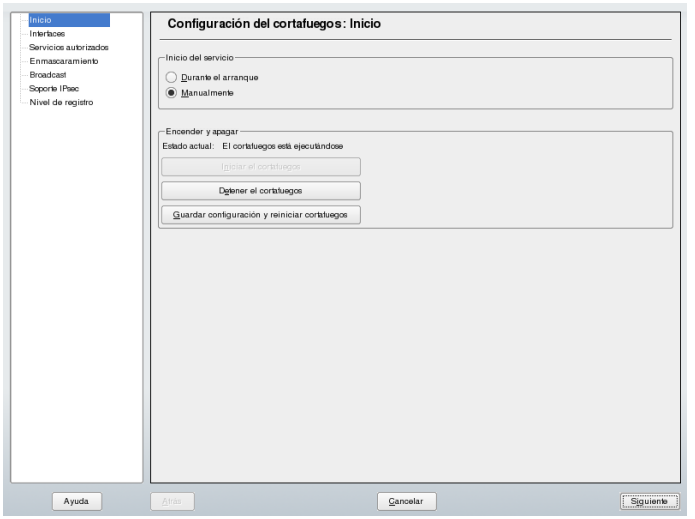
IMPORTANTE: Configuración automática del cortafuegos

Después de la instalación, YaST iniciará de forma automática un cortafuegos en todas las interfaces configuradas. Si se configura y se activa un servidor en el sistema, YaST puede modificar la configuración del cortafuegos que se ha generado automáticamente mediante las opciones *Open Ports on Selected Interface in Firewall* (Abrir puertos en la interfaz seleccionada del cortafuegos) o *Open Ports on Firewall* (Abrir puertos en el cortafuegos) de los módulos de configuración del servidor. Algunos cuadros de diálogo del módulo del servidor incluyen un botón denominado *Detalles del cortafuegos* que permite activar servicios y puertos adicionales. El módulo de configuración del cortafuegos de YaST se puede utilizar para activar, desactivar o volver a configurar el cortafuegos.

Se puede acceder a los cuadros de diálogo de YaST para la configuración gráfica a través del Centro de Control de YaST. Seleccione *Seguridad y usuarios* → *Cortafuegos*. La configuración se divide en siete secciones a las que se puede acceder directamente desde la estructura de árbol que se encuentra situada en la parte izquierda del cuadro de diálogo.

Inicio
: Defina el comportamiento de inicio en este cuadro de diálogo. Cuando se trate de una instalación por defecto, SuSEfirewall2 se iniciará automáticamente. También puede iniciar aquí tanto el inicio como la detención del cortafuegos. Para implementar la nueva configuración en un cortafuegos que se esté ejecutando, utilice la opción *Guardar la configuración y reiniciar cortafuegos*.

Figura 4.2 *Configuración de cortafuegos de YaST*



Interfaces

En este cuadro de diálogo se muestra una lista con todas las interfaces de red conocidas. Para eliminar una interfaz de una zona, seleccione la interfaz y, a continuación, pulse *Cambiar* y seleccione *Ninguna zona asignada*. Para añadir una interfaz a una zona, seleccione la interfaz, pulse *Cambiar* y, a continuación, seleccione cualquiera de las zonas disponibles. También puede crear una interfaz especial con sus propios ajustes utilizando para ello la opción *Personalizar*.

Servicios autorizados

Esta opción es necesaria para poder ofrecer servicios desde su sistema a una zona que se encuentre protegida. Por defecto, el sistema se encuentra protegido únicamente de zonas externas. Autorice expresamente los servicios que deberían estar disponibles para los hosts externos. Active los servicios después de seleccionar la zona deseada en *Allowed Services for Selected Zone* (Servicios autorizados para zona seleccionada).

Enmascaramiento

El enmascaramiento oculta su red interna a las redes externas, como por ejemplo Internet, al tiempo que permite que los hosts de la red interna puedan acceder a la red externa de forma transparente. Las solicitudes enviadas de la red externa a la red interna se bloquean, mientras que las solicitudes enviadas por la red interna parecen ser enviadas por el servidor de enmascaramiento cuando éstas se ven

externamente. Si los servicios especiales de una máquina interna necesitan estar disponibles para la red externa, añada reglas especiales de redirección para el servicio.

Broadcast
: En este cuadro de diálogo, configure los puertos UDP que permiten difusiones. Añada los números o servicios de puertos necesarios a la zona adecuada, separados entre sí por espacios. Consulte igualmente el archivo `/etc/services`.

  Es aquí, por otra parte, donde puede habilitarse el registro de las difusiones no aceptadas. Esto puede originar problemas, puesto que los hosts de Windows utilizan difusiones para saber obtener información unos de otros y, de esa forma, generan paquetes que no son aceptados.

Soporte IPsec
: Determine si el servicio IPsec deberá estar disponible para la red externa en este cuadro de diálogo. Configure qué paquetes son confiables en *Detalles*.

Nivel de registro
: Son dos las reglas existentes para el registro: paquetes aceptados y no aceptados. Los paquetes no aceptados son DROPPED (SUPRIMIDOS) o REJECTED (RECHAZADOS). Seleccione para ambos una de las siguientes opciones: *Registrar todos*, *Log Critical* (Registrar críticos) o *No registrar ninguno*.

Una vez que haya concluido la configuración del cortafuegos, salga de este cuadro de diálogo utilizando la opción *Siguiente*. Se abrirá a continuación un resumen de la configuración de su cortafuegos orientado a las zonas. En dicho resumen, compruebe todos los ajustes. Todos los servicios, puertos y protocolos que se han autorizado se indican en este resumen. Para modificar la configuración, utilice la opción *Atrás*. Pulse *Aceptar* para guardar su configuración.

Configuración manual

Los párrafos que aparecen a continuación ofrecen instrucciones detalladas para lograr una configuración adecuada. Cada elemento de la configuración se marca siempre y cuando sea relevante para los cortafuegos o el enmascaramiento. Los aspectos relacionados con la DMZ (zona desmilitarizada), de acuerdo con lo mencionado en el archivo de configuración, no se cubren en esta sección. Estos aspectos son de aplicación únicamente en infraestructuras de redes más complejas localizadas en organizaciones

de mayor tamaño (redes corporativas), que precisan una configuración ampliada y un conocimiento exhaustivo sobre el tema.

En primer lugar, emplee los Servicios del sistema (niveles de ejecución) del módulo YaST para habilitar SuSEfirewall2 en su nivel de ejecución (3 ó 5 con mayor probabilidad). Los enlaces simbólicos para los guiones de SuSEfirewall2_* se establecen en los directorios `/etc/init.d/rc?.d/`.

`FW_DEV_EXT` (cortafuegos, enmascaramiento)
: Es el dispositivo que está conectado a Internet. Para una conexión por módem, escriba `ppp0`. Para una conexión RDSI, utilice `ippp0`. Las conexiones DSL, por su parte, utilizan `dsl0`. Especifique `auto` para utilizar la interfaz que se corresponda con la ruta por defecto.

`FW_DEV_INT` (cortafuegos, enmascaramiento)
: Es el dispositivo conectado a la red interna privada (como por ejemplo `eth0`). Deje esta opción en blanco si no existe una red interna y si el cortafuegos protege solamente el host en el que se ejecuta el cortafuegos.

`FW_ROUTE` (cortafuegos, enmascaramiento)
: Si precisa la función de enmascaramiento, fije este valor en `yes`. Sus hosts internos no serán visibles desde el exterior, debido a que sus direcciones de redes privadas (como, por ejemplo, `192.168.x.x`) no son tenidas en cuenta por los routers de Internet.

  Para un cortafuegos sin enmascaramiento, únicamente fije este valor en `yes` si quiere permitir el acceso a la red interna. Sus hosts internos necesitan utilizar únicamente IPs registradas en este caso. Por norma general, sin embargo, se recomienda que *no* permita el acceso a su red interna desde el exterior.

`FW_MASQUERADE` (enmascaramiento)
: Establezca este valor en `yes` si precisa la función de enmascaramiento. Esto proporciona a los hosts internos una conexión prácticamente directa a Internet. Es más seguro contar con un servidor alterno entre los hosts de la red interna e Internet. El enmascaramiento no es necesario para aquellos servicios proporcionados por servidores alternos.

`FW_MASQ_NETS` (enmascaramiento)
: Especifique los hosts o las redes para las que se realizará el enmascaramiento; no olvide dejar un espacio entre cada una de las entradas individuales. Por ejemplo:

```
FW_MASQ_NETS="192.168.0.0/24 192.168.10.1"
```

FW_PROTECT_FROM_INT (cortafuegos)
: Establezca este valor en `yes` para proteger el host del cortafuegos frente a ataques originados en la red interna. Los servicios estarán disponibles para la red interna únicamente si se han habilitado expresamente. A este respecto, consulte también FW_SERVICES_INT_TCP y FW_SERVICES_INT_UDP.

FW_SERVICES_EXT_TCP (cortafuegos)
: Introduzca los puertos TCP que deberían estar disponibles. Deje esta opción en blanco en aquellas estaciones de trabajo normales de uso doméstico que no se emplean para ofrecer servicios.

FW_SERVICES_EXT_UDP (cortafuegos)
: Deje esta opción en blanco excepto si se ejecuta un servicio UDP y quiere que se pueda acceder a él desde el exterior. Los servicios que emplean UDP incluyen, entre otros, a los servidores DNS, IPSec, TFTP y DHCP. En ese caso, escriba los puertos UDP que se van a emplear.

FW_SERVICES_INT_TCP (cortafuegos)
: Defina con esta variable los servicios disponibles para la red interna. La notación es la misma que la empleada en FW_SERVICES_EXT_TCP, pero en este caso los ajustes se aplican a la red *interna*. La variable solamente necesita establecerse si FW_PROTECT_FROM_INT se ha fijado en el valor `yes`.

FW_SERVICES_INT_UDP (cortafuegos)
: Consulte FW_SERVICES_INT_TCP.

Después de haber configurado el cortafuegos, compruebe la configuración del dispositivo. Los conjuntos de reglas del cortafuegos se crean escribiendo el comando `SuSEfirewall2 start` como usuario `root`. A continuación, utilice por ejemplo el comando `telnet` desde un host externo para comprobar si se ha denegado la conexión. Después de esta operación, consulte `/var/log/messages`, donde debería aparecer un mensaje como el que se muestra a continuación:

```
Mar 15 13:21:38 linux kernel: SFW2-INext-DROP-DEFLT IN=eth0
OUT= MAC=00:80:c8:94:c3:e7:00:a0:c9:4d:27:56:08:00 SRC=192.168.10.0
DST=192.168.10.1 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=15330 DF PROTO=TCP
SPT=48091 DPT=23 WINDOW=5840 RES=0x00 SYN URGP=0
OPT (020405B40402080A061AFEBC0000000001030300)
```

Otros paquetes que le permitirán probar la configuración del cortafuegos son nmap o nessus. Después de instalar los paquetes respectivos, la documentación de nmap se

encuentra en /usr/share/doc/packages/nmap, mientras que la documentación de nessus se localiza en el directorio /usr/share/doc/packages/nessus-core.

4.1.5 Información adicional

La información más actualizada y la documentación adicional acerca del paquete SuSEfirewall2 se encuentra en /usr/share/doc/packages/SuSEfirewall2. La página Web del proyecto netfilter y iptables, http://www.netfilter.org, ofrece un amplio catálogo de documentos disponibles en diversas lenguas.

4.2 SSH: operaciones de red seguras

Dado el creciente número de equipos instalados en entornos de red, a menudo es preciso acceder a los hosts desde una ubicación remota, lo que normalmente conlleva que el usuario envíe cadenas de inicio de sesión y de contraseña con fines de autenticación. Si esas cadenas se transmiten como texto sin formato, pueden ser interceptadas y usadas de forma fraudulenta para acceder a la cuenta de ese usuario sin que el usuario autorizado ni siquiera tenga constancia de ello. Aparte del hecho de que de este modo el atacante tendría libre acceso a todos los archivos del usuario, la cuenta fraudulenta se podría utilizar para obtener acceso de administrador o de usuario Root o para acceder a otros sistemas. En el pasado, las conexiones remotas se establecían a través de telnet, que no ofrece garantías contra el acceso no autorizado mediante el cifrado ni ningún otro mecanismo de seguridad. Existen otros canales de comunicación no protegida, como el protocolo FTP tradicional y algunos programas de copia remotos.

El paquete SSH proporciona la protección necesaria mediante el cifrado de las cadenas de autenticación (por lo general, un nombre de inicio de sesión y una contraseña) y de todos los demás datos que se intercambian entre los hosts. Con SSH, los usuarios externos pueden seguir registrando el flujo de los datos, pero el contenido se cifra y no se puede convertir a texto sin formato a menos que se conozca la clave de cifrado. Por tanto, SSH habilita la comunicación segura en redes no seguras, como Internet. El tipo de SSH que acompaña a SUSE Linux es OpenSSH.

4.2.1 Paquete OpenSSH

Con SUSE Linux se instala el paquete OpenSSH por defecto. Con él, los programas ssh, scp y sftp están disponibles como alternativas de telnet, rlogin, rsh, rcp y ftp. En la configuración por defecto, el acceso al sistema en SUSE Linux sólo es posible mediante las utilidades de OpenSSH y únicamente si el cortafuegos lo permite.

4.2.2 Programa ssh

Gracias al programa ssh, es posible iniciar la sesión en sistemas remotos y trabajar de modo interactivo. Sustituye tanto a telnet como a rlogin. El programa slogin es sólo un enlace simbólico que señala a ssh. Por ejemplo, se puede iniciar la sesión en un host llamado sun con el comando `ssh sun`. El host solicita entonces la contraseña para el host sun.

Una vez que se autentique correctamente, podrá trabajar en la línea de comandos remota o utilizar aplicaciones interactivas, como YaST. Si el nombre de usuario local es distinto del remoto, puede iniciar la sesión con un nombre de inicio de sesión distinto mediante `ssh -l augustine sun` o bien `ssh augustine@sun`.

Además, ssh ofrece la posibilidad de ejecutar comandos en sistemas remotos, igual que con rsh. En el siguiente ejemplo, se ejecuta el comando `uptime` en el host sun y se crea un directorio denominado `tmp`. La salida del programa se muestra en el terminal local del host earth.

```
ssh otherplanet "uptime; mkdir tmp"
tux@otherplanet's password:
1:21pm  up  2:17,  9 users,  load average: 0.15, 0.04, 0.02
```

Las comillas son precisas para enviar ambas instrucciones con un comando. Sólo así se consigue que el segundo comando se ejecute en el host sun.

4.2.3 scp: copia segura

scp permite copiar archivos a un equipo remoto. Constituye una alternativa segura y cifrada de rcp. Por ejemplo, con `scp MiCarta.tex sun:` se copia el archivo `MiCarta.tex` del host earth al host sun. Si el nombre de usuario del host earth es distinto del nombre de usuario del host sun, se debe especificar este último con el formato `nombreusuario@host`. Este comando no cuenta con la opción `-l`.

Una vez que se introduce la contraseña correcta, scp inicia la transferencia de datos y muestra una fila de asteriscos que va aumentando para simular una barra de progreso. Además, el programa muestra el tiempo estimado que queda para que se complete esa barra de progreso. Puede suprimir la salida incluyendo la opción `-q`.

scp proporciona también una función de copia reiterativa apropiada para directorios completos. Con el comando `scp -r src/ sun:backup/` se copia todo el contenido del directorio `src`, incluidos todos los subdirectorios, al directorio `backup` del host sun. Si este directorio no existe, se crea automáticamente.

La opción `-p` indica a scp que debe mantener intacta la marca horaria de los archivos. Con la opción `-C`, se comprime la transferencia de datos. De este modo se reduce al mínimo el volumen de datos que se deben transferir, pero se genera una carga mayor en el procesador.

4.2.4 sftp: transferencia de archivos segura

El programa sftp se puede utilizar en lugar de scp para la transferencia de archivos segura. Durante una sesión de sftp se pueden utilizar muchos de los comandos de ftp conocidos. sftp puede ser más apropiado que scp, especialmente cuando se transfieren datos cuyos nombres de archivo se desconocen.

4.2.5 Daemon SSH (sshd): servidor

Para utilizar los programas de cliente SSH ssh y scp, se debe estar ejecutando en segundo plano un servidor, el daemon SSH, que debe estar a la escucha de las conexiones en el `puerto TCP/IP 22`. El daemon genera tres pares de claves cuando se inicia por primera vez. Cada par está integrado por una clave privada y una pública, por lo que se habla de este procedimiento como un procedimiento basado en claves públicas. Para garantizar la seguridad de la comunicación a través de SSH, se debe restringir el acceso a los archivos de claves privadas al administrador del sistema. Los permisos de archivo se definen convenientemente en la instalación por defecto. Las claves privadas se necesitan sólo de forma local para el daemon SSH y no se deben proporcionar a ningún otro usuario. Los componentes de claves públicas (reconocibles por la extensión de nombre `.pub`) se envían al cliente que solicita la conexión y pueden leerlos todos los usuarios.

El cliente SSH inicia una conexión. El daemon SSH a la espera y el cliente SSH solicitante intercambian datos de identificación para comparar las versiones del protocolo y del software y para impedir las conexiones a través de un puerto equivocado. Dado que a la solicitud responde un proceso secundario del daemon SSH original, se pueden establecer varias conexiones SSH al mismo tiempo.

Para la comunicación entre el servidor y el cliente SSH, OpenSSH es compatible con las versiones 1 y 2 del protocolo SSH. En los sistemas SUSE Linux que se hayan instalado recientemente, la versión por defecto es la 2. Para seguir utilizando la versión 1 después de actualizar, siga las instrucciones detalladas en `/usr/share/doc/packages/openssh/README.SuSE`. En ese documento se describe también la forma de transformar un entorno SSH 1 en un entorno SSH 2 en funcionamiento en unos pocos pasos.

Cuando se utiliza la versión 1 de SSH, el servidor envía su clave de host pública y una clave de servidor, que se genera en el daemon SSH cada hora. Ambas claves permiten que el cliente cifre una clave de sesión que se elige libremente y que se envía al servidor SSH. El cliente SSH indica además al servidor el método de cifrado que se debe utilizar.

La versión 2 del protocolo SSH no requiere una clave de servidor. En ambos extremos se emplea un algoritmo Diffie-Helman para intercambiar las claves.

Las claves de host privada y de servidor son absolutamente necesarias para descifrar la clave de sesión y no se pueden obtener a partir de las partes públicas. Sólo el daemon SSH con el que se contacta puede descifrar la clave de sesión utilizando sus claves privadas (consulte `man /usr/share/doc/packages/openssh/RFC.nroff`). Esta fase inicial de la conexión se puede vigilar de cerca activando la opción de depuración detallada `-v` del cliente SSH.

La versión 2 del protocolo SSH se utiliza por defecto. Se puede anular esta configuración y utilizar la versión 1 del protocolo con el conmutador `-1`. El cliente almacena todas las claves públicas del host en `~/.ssh/known_hosts`, después de establecer el primer contacto con un host remoto. De esta forma se evitan los ataques por parte de intrusos: intentos de servidores SSH extraños de utilizar nombres y direcciones IP de suplantación. Este tipo de ataques se detectan mediante una clave de host que no está incluida en `~/.ssh/known_hosts` o por la imposibilidad del servidor de descifrar la clave de sesión al no encontrarse la clave privada correspondiente adecuada.

Se recomienda guardar una copia de seguridad de las claves privadas y públicas almacenadas en `/etc/ssh/` en una ubicación externa segura, con el fin de detectar

modificaciones de las claves y volver a utilizar las anteriores después de realizar una instalación nueva. De este modo, se ahorra a los usuarios las advertencias perturbadoras. Si se comprueba que, a pesar de la advertencia, se trata en realidad del servidor SSH correcto, la entrada existente para el sistema se debe eliminar de `~/.ssh/known_hosts`.

4.2.6 Mecanismos de autenticación de SSH

A continuación, tiene lugar la autenticación en sí, la cual, en su forma más básica, consiste en introducir una contraseña como se ha mencionado arriba. SSH obedece a la necesidad de introducir un software seguro que resulte además fácil de utilizar. Dado que está pensado para sustituir a rsh y a rlogin, SSH debe ser capaz también de proporcionar un método de autenticación adecuado para el uso cotidiano, lo que se consigue por medio de otro par de claves que genera el usuario. El paquete SSH proporciona un programa de ayuda para ello: ssh-keygen. Tras introducir `ssh-keygen -t rsa` o `ssh-keygen -t dsa`, se genera el par de claves y se pide al usuario que proporcione un nombre de archivo de base en el que almacenar las claves.

Confirme el ajuste por defecto y responda a la solicitud de contraseña codificada. Incluso cuando el software sugiere una contraseña codificada vacía, se recomienda utilizar un texto de una longitud comprendida entre 10 y 30 caracteres para el procedimiento descrito aquí. No utilice palabras o frases cortas y sencillas. Confirme la acción repitiendo la contraseña codificada. A continuación, verá la ubicación donde se almacenan las claves pública y privada. En este ejemplo, en los archivos `id_rsa` y `id_rsa.pub`.

Utilice `ssh-keygen -p -t rsa` o `ssh-keygen -p -t dsa` para cambiar la contraseña codificada anterior. Copie el componente de clave pública (`id_rsa.pub` en el ejemplo) en el equipo remoto y guárdelo en `~/.ssh/authorized_keys`. Se le pedirá que se autentique con su contraseña codificada cuando vuelva a establecer una conexión. Si no es así, compruebe la ubicación y el contenido de esos archivos.

A la larga, este procedimiento resulta más engorroso que proporcionar la contraseña cada vez. Por eso, el paquete SSH proporciona otra herramienta, ssh-agent, que mantiene las claves privadas mientras dure una sesión X. La sesión X se inicia como un proceso secundario de ssh-agent. La forma más fácil de llevar a cabo este procedimiento consiste en definir la variable `usessh` al principio del archivo `.xsession` con el valor `yes`

(sí) e iniciar la sesión mediante un gestor de pantalla, como KDM o XDM. Del mismo modo, también puede introducir `ssh-agent startx`.

En este momento, puede utilizar ssh o scp como de costumbre. Si ha distribuido su clave pública como se describe arriba, ya no se le solicitará la contraseña. Asegúrese de terminar la sesión X o de bloquearla con una aplicación de protección de contraseña, como xlock.

Todos los cambios pertinentes derivados de la introducción de la versión 2 del protocolo SSH están también documentados en el archivo `/usr/share/doc/packages/openssh/README.SuSE`.

4.2.7 Mecanismos X, de autenticación y remisión

Más allá de las mejoras relacionadas con la seguridad descritas anteriormente, SSH también simplifica el uso de aplicaciones X remotas. Si ejecuta `ssh` con la opción `-X`, la variable DISPLAY se define automáticamente en el equipo remoto y toda la salida de X se exporta al equipo remoto a través de la conexión SSH existente. Al mismo tiempo, las aplicaciones X que se inician de forma remota y se ven localmente con este método no pueden ser interceptadas por usuarios no autorizados.

Si se añade la opción `-A`, el mecanismo de autenticación de ssh-agent se transfiere a la siguiente máquina. De este modo, puede trabajar desde distintas máquinas sin necesidad de escribir la contraseña, pero sólo si ha distribuido su clave pública a los hosts de destino y la ha almacenado correctamente en ellos.

Ambos mecanismos están desactivados en los ajustes por defecto, pero se pueden activar de forma permanente en cualquier momento en el archivo de configuración del sistema, `/etc/ssh/sshd_config`, o en el del usuario, `~/.ssh/config`.

ssh también se puede utilizar para redirigir conexiones TCP/IP. En los ejemplos siguientes, se le indica a SSH que debe redirigir el puerto SMTP y el puerto POP3, respectivamente:

```
ssh -L 25:sun:25 earth
```

Con este comando, cualquier conexión dirigida al puerto 25 (SMTP) del host earth se redirige al puerto SMTP del host sun a través de un canal cifrado. Esto resulta especialmente útil para quienes utilicen servidores SMTP sin las funciones SMTP-

AUTH o POP antes de SMTP. Desde cualquier ubicación arbitraria conectada a una red, se puede transferir el correo electrónico al servidor de correo "personal" para su distribución. Del mismo modo, todas las solicitudes POP3 (puerto 110) del host earth se pueden remitir al puerto POP3 del host sun con este comando:

```
ssh -L 110:sun:110 earth
```

Ambos comandos se deben ejecutar como usuario `Root`, debido a que la conexión se establece con puertos locales que requieren privilegios. El correo electrónico se envía y se recupera por parte de los usuarios normales a través de una conexión SSH existente. Los hosts SMTP y POP3 se deben definir como `localhost` para que esto funcione. Para obtener información adicional, consulte las páginas Man de cada uno de los programas descritos arriba o los archivos incluidos en `/usr/share/doc/packages/openssh`.

4.3 Cifrado de particiones y archivos

Todo usuario tiene algún dato confidencial que no debería estar al alcance de terceros. Cuantas más conexiones y más movilidad tenga un equipo, con más cuidado deben tratarse los datos. Se recomienda el cifrado de archivos o de particiones enteras si hay terceros que puedan obtener acceso físico o a través de la red.

AVISO: El cifrado de medios ofrece una protección limitada

Tenga en cuenta que mediante los métodos descritos en esta sección no es posible proteger un equipo en funcionamiento. Una vez montado correctamente un medio cifrado, cualquier usuario con los permisos correspondientes tendrá acceso a él. El cifrado de medios es útil si el equipo se pierde o lo roban y usuarios sin autorización intentan leer datos confidenciales.

A continuación aparecen algunas situaciones posibles de uso.

Equipos portátiles
: Si se viaja con un equipo portátil, es buena idea cifrar las particiones del disco duro que contengan datos confidenciales. Si pierde el equipo o se lo roban, nadie podrá acceder a los datos que se encuentren en un sistema de archivos cifrado o en un archivo independiente cifrado.

Medios extraíbles
: Las unidades flash USB o los discos duros externos son tan susceptibles de robo como los equipos portátiles. Un sistema de archivos cifrado ofrece protección frente al acceso de terceros.

Estaciones de trabajo
: En entornos empresariales en los que muchas personas tienen acceso a los equipos, puede resultar útil cifrar particiones o archivos independientes.

4.3.1 Configuración de un sistema de archivos cifrado con YaST

YaST ofrece cifrado de archivos y particiones durante la instalación así como en sistemas ya instalados. Los archivos cifrados se pueden crear en cualquier momento porque se integran perfectamente en la distribución de particiones. Para cifrar una partición entera, dedique una partición a cifrado en la distribución de particiones. La propuesta de distribución de particiones estándar que YaST sugiere por defecto no incluye una partición cifrada. Añádala manualmente en el cuadro de diálogo de particionamiento.

Creación de una partición cifrada durante la instalación

AVISO: Introducción de contraseñas

Cuando establezca contraseñas para particiones cifradas, tenga en cuenta los avisos de seguridad y memorícelas bien. Sin la contraseña no se puede acceder a los datos cifrados ni restaurarlos.

El cuadro de diálogo de particionamiento avanzado de YaST, que se describe en la Sección “Particionamiento” (Capítulo 2, *Configuración del sistema con YaST*, ↑Inicio), ofrece las opciones necesarias para crear particiones cifradas. Haga clic en *Crear* como al crear particiones normales. En el cuadro de diálogo que se abre, introduzca los parámetros de la nueva partición, como por ejemplo, el formato deseado y el punto de montaje. Complete el proceso haciendo clic en *Sistema de archivos codificado*. En el siguiente cuadro de diálogo, introduzca dos veces la contraseña. La nueva partición cifrada se creará al cerrar el cuadro de diálogo de particionamiento haciendo clic en

Aceptar. Al arrancar, el sistema operativo solicitará la contraseña antes de montar la partición.

Si no desea montar la partición cifrada durante el inicio, pulse Entrar cuando se le pida la contraseña. A continuación, rechace la posibilidad de volver a introducir la contraseña. En este caso, el sistema de archivos cifrado no se montará y el sistema operativo continuará iniciándose, pero el acceso a los datos estará bloqueado. Una vez montada, todos los usuarios podrán acceder a la partición.

Si el sistema de archivos cifrado sólo debe montarse cuando sea necesario, active la opción *Do Not Mount During Booting* (No montar durante el arranque) en el cuadro de diálogo *Opciones fstab*. La partición correspondiente no se montará cuando se arranque el sistema. Después, para que sea accesible, móntela manualmente con `mount nombre_de_la_particion punto_de_montaje`. Introduzca la contraseña cuando se le pida. Cuando acabe de trabajar con la partición, desmóntela con `unmount nombre_de_la_particion` para impedir el acceso de otros usuarios.

Creación de una partición cifrada en un sistema en funcionamiento

AVISO: Activación del cifrado en un sistema en funcionamiento

También es posible crear particiones cifradas en un sistema en funcionamiento durante la instalación. Sin embargo, el cifrado de una partición existente destruye todos los datos que contenga.

En un sistema en funcionamiento, seleccione *Sistema → Particionamiento* en el centro de control de YaST. Haga clic en *Sí* para continuar. En lugar de seleccionar *Crear* como se describía anteriormente, haga clic en *Editar*. El resto del procedimiento es igual.

Instalación de archivos cifrados

En lugar de utilizar una partición, es posible crear sistemas de archivos cifrados dentro de archivos independientes para almacenar datos confidenciales. Estos se crean desde el mismo cuadro de diálogo de YaST. Seleccione *Archivo crypt* e introduzca la vía al archivo que se creará y el tamaño deseado. Acepte la configuración de formato propuesta

y el tipo de sistema de archivos. A continuación, especifique el punto de montaje y decida si el sistema de archivos cifrados debe montarse cuando se arranque el sistema.

La ventaja de los archivos cifrados es que se pueden añadir sin volver a particionar el disco duro. Se montan mediante un dispositivo de bucle y tienen el mismo comportamiento que una partición normal.

Uso de vi para cifrado de archivos

La desventaja de utilizar particiones cifradas es que, mientras la partición se encuentre montada, como mínimo el usuario `root` podrá acceder a los datos. Para evitarlo, se puede utilizar vi en modo cifrado.

Utilice `vi -x` *`nombre_del_archivo`* para editar un archivo nuevo. vi solicitará que se establezca una contraseña, tras lo cual cifrará el contenido del archivo. Cada vez que se acceda al archivo, vi solicitará la contraseña correspondiente.

Si se desea una seguridad todavía mayor, es posible ubicar el archivo de texto cifrado en una partición cifrada. Se recomienda hacerlo dado que el cifrado utilizado en vi no es muy fuerte.

4.3.2 Cifrado del contenido de medios extraíbles

YaST trata los medios extraíbles, tales como discos duros externos o unidades flash USB, de la misma manera que cualquier disco duro. Los archivos o las particiones de estos medios pueden cifrarse de la manera anteriormente descrita. Sin embargo, seleccione que estos medios no se monten durante el inicio del sistema, dado que normalmente sólo se conectan mientras el sistema se encuentra funcionando.

4.4 Limitación de privilegios con AppArmor

Muchas vulnerabilidades de seguridad se producen por fallos en los programas *de confianza.* Los programas *de confianza* se ejecutan con privilegios que algunos atacantes

desean tener, por lo que ese programa deja de ser de confianza si tiene un fallo que permita al atacante conseguir esos privilegios.

Novell® AppArmor es una solución de seguridad de aplicaciones diseñada específicamente para reducir al mínimo los privilegios de los programas sospechosos. AppArmor permite al administrador especificar el dominio de actividades que el programa puede realizar desarrollando un *perfil* de seguridad para esa aplicación, que consiste en una lista de archivos a los que puede acceder el programa y las acciones que puede llevar a cabo.

El robustecimiento de un sistema informático requiere la reducción al mínimo del número de programas que otorgan privilegios y, seguidamente, la aplicación de toda la seguridad posible a los programas. Con Novell AppArmor, lo único que necesita es definir el perfil de los programas que están expuestos a ataques en su entorno, con lo que se reduce drásticamente la cantidad de trabajo necesario para robustecer el equipo. Los perfiles de AppArmor aplican directivas que garantizan que los programas hacen lo que se supone que deben hacer, pero nada más.

Los administradores sólo tienen que preocuparse de las aplicaciones vulnerables a los ataques y generar perfiles para ellas. El robustecimiento de un sistema, por lo tanto, se reduce a crear y mantener el conjunto de perfiles de AppArmor y a monitorizar las violaciones de las directivas o las excepciones registradas por la utilidad de creación de informes de AppArmor.

La creación de perfiles de AppArmor con los que limitar las aplicaciones es muy directa e intuitiva. AppArmor se distribuye con varias herramientas que asisten en la creación de perfiles. AppArmor no requiere ninguna tarea de programación ni de gestión de guiones. La única tarea que deberá realizar el administrador es establecer una directiva del acceso más estricto y ejecutar permisos para cada aplicación que deba controlarse.

La actualización o la modificación de los perfiles de aplicaciones sólo son precisas cuando cambia la configuración del software o el ámbito de actividades necesario. AppArmor ofrece herramientas intuitivas para gestionar la actualización y la modificación de los perfiles.

Los usuarios no notarán en absoluto la presencia de AppArmor. Se ejecuta “en segundo plano” y no requiere ningún tipo de interacción por parte del usuario. El rendimiento tampoco se verá afectado de forma perceptible por el uso de AppArmor. Si alguna actividad de la aplicación no queda cubierta por un perfil de AppArmor, o si se impide alguna actividad, el administrador tendrá que ajustar el perfil de esa aplicación para que cubra ese tipo de comportamiento.

En esta guía se describen las tareas básicas que hay que llevar a cabo con AppArmor para proteger el sistema de forma eficaz. Para obtener información más detallada, consulte la *Guía de administración de Novell AppArmor 2.0.*

4.4.1 Instalación de Novell AppArmor

Los usuarios que opten por la instalación de un escritorio GNOME o KDE pueden omitir esta sección, ya que Novell AppArmor se instala por defecto con esas opciones.

Si no instala ninguno de estos escritorios, o incluso si va a instalar un entorno basado totalmente en texto, haga lo siguiente para instalar los paquetes necesarios utilizando el gestor de paquetes de YaST.

1. Inicie la sesión como usuario `Root` y abra YaST.

2. En el Centro de control de YaST, seleccione *Software → Instalar/desinstalar software.*

3. Utilice la función de búsqueda de YaST (palabra clave “AppArmor”) para instalar los siguientes paquetes:

   - apparmor-parser
   - libapparmor
   - apparmor-docs
   - yast2-apparmor
   - apparmor-profiles
   - apparmor-utils

4. Seleccione todos esos paquetes para instalarlos y después elija *Aceptar.* YaST resuelve todas las dependencias e instala todos los paquetes sin que el usuario tenga que intervenir.

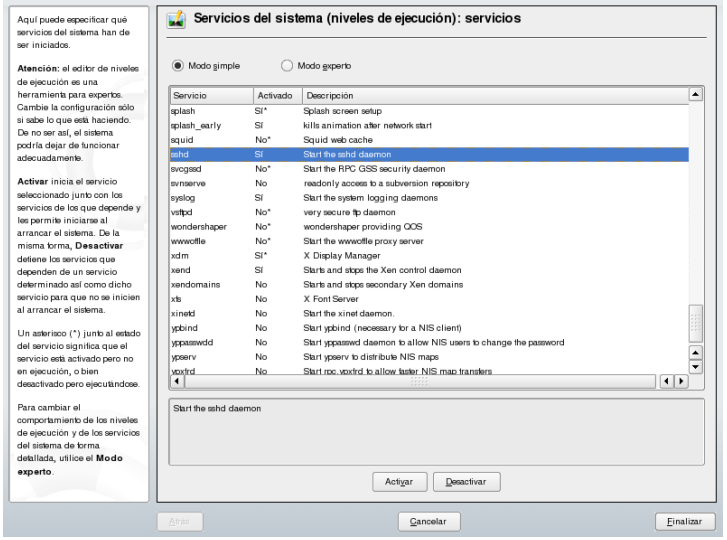
5. Cuando YaST haya terminado de actualizar la configuración del sistema, haga clic en *Finalizar* para salir del gestor de paquetes.

4.4.2 Habilitación de Novell AppArmor

Cuando se haya instalado Novell AppArmor, habilítelo explícitamente para asegurarse de que se iniciará cuando se abra el sistema. Utilice el módulo Servicios del sistema (niveles de ejecución) de YaST para esta tarea:

1. Inicie la sesión como usuario `Root` y abra YaST.
2. Abra *Sistema* → *Servicios del sistema* (Niveles de ejecución).
3. En la lista de servicios mostrada, seleccione `apparmor`. Consulte la Figura 4.3, “Habilitación de Novell AppArmor con YaST” (p. 133).
4. Haga clic en *Habilitar* para habilitar AppArmor de forma permanente.
5. Haga clic en *Finalizar* para aceptar los ajustes.

Figura 4.3 *Habilitación de Novell AppArmor con YaST*



Mediante la herramienta de niveles de ejecución de YaST, es posible habilitar de forma permanente los servicios: estos ajustes se mantienen tras rearrancar el sistema. Para habilitar AppArmor de forma temporal (únicamente mientras dure una sesión), haga lo siguiente:

1 Inicie la sesión como usuario `Root` y abra YaST.

2 Inicie *Novell AppArmor → Panel de control de AppArmor.*

3 Defina la opción *Estado de AppArmor* con el valor *AppArmor está habilitado* haciendo clic en *Configurar → Habilitar → Aceptar.*

4 Confirme sus ajustes con la opción *Terminado.*

4.4.3 Procedimientos iniciales para la creación de perfiles de aplicaciones

Para preparar una instalación correcta de Novell AppArmor en el sistema, tenga especial cuidado con los siguientes elementos:

1 Determine las aplicaciones para las que hay que crear perfiles. Obtenga más información al respecto en "Selección de las aplicaciones para las que crear perfiles" (p. 134).

2 Cree los perfiles necesarios como se describe de forma somera en "Creación y modificación de perfiles" (p. 135). Compruebe los resultados y ajuste los perfiles según sea necesario.

3 Haga un seguimiento de lo que ocurre en el sistema ejecutando informes de AppArmor y resolviendo los eventos de seguridad. Consulte "Configuración de notificaciones de eventos e informes de Novell AppArmor" (p. 138).

4 Actualice los perfiles cuando se produzcan cambios en el entorno o cuando tenga que reaccionar a los eventos de seguridad registrados por la herramienta de informes de AppArmor. Consulte "Actualización de los perfiles" (p. 139).

Selección de las aplicaciones para las que crear perfiles

Sólo es necesario proteger los programas que están expuestos a ataques con su configuración concreta, por lo tanto, sólo se usarán los perfiles de las aplicaciones que se ejecuten realmente. Utilice la siguiente lista para determinar los candidatos más probables:

Agentes de red
: Los programas (servidores y clientes) tienen puertos de red abiertos y los agentes de red son programas servidores que responden a esos puertos. Los clientes de los usuarios (por ejemplo, los clientes de correo electrónico o los navegadores Web) también tienen puertos de red abiertos y otorgan privilegios.

Aplicaciones Web
: Los guiones CGI de Perl, las páginas PHP y aplicaciones Web mucho más complejas se pueden invocar mediante un navegador Web.

Tareas del daemon cron
: Los programas que ejecuta periódicamente el daemon cron leen datos de entrada de varios orígenes.

Para averiguar qué procesos se están ejecutando actualmente con puertos de red abiertos y pueden requerir un perfil que los limite, ejecute el comando `unconfined` como usuario `Root.`

Ejemplo 4.1 *Resultado del comando unconfined*

```
19848 /usr/sbin/cupsd not confined
19887 /usr/sbin/sshd not confined
19947 /usr/lib/postfix/master not confined
29205 /usr/sbin/sshd confined by '/usr/sbin/sshd (enforce)'
```

Todos los procesos del ejemplo anterior con la etiqueta `not confined` (sin limitar) pueden requerir un perfil personalizado para limitarlos. Los indicados con la etiqueta `confined by` (limitado por) ya están protegidos por AppArmor.

SUGERENCIA: Información adicional

Para obtener más información acerca de cómo elegir las aplicaciones que necesitan perfiles, consulte el capítulo *Selección de programas que inmunizar (Guía de administración de Novell AppArmor 2.0)*.

Creación y modificación de perfiles

Novell AppArmor en SUSE Linux incluye un conjunto preconfigurado de perfiles para las aplicaciones más importantes. Asimismo, puede utilizar AppArmor para crear sus propios perfiles para un conjunto de aplicaciones definido en `/etc/apparmor/README.profiles`.

Existen dos formas de gestionar perfiles. Una consiste en utilizar la interfaz gráfica ofrecida por los módulos de Novell AppArmor de YaST; la otra es utilizar las herramientas de la línea de comandos ofrecidas por el propio paquete de AppArmor. Ambos métodos funcionan básicamente igual.

Si se ejecuta sin limitación, como se describe en "Selección de las aplicaciones para las que crear perfiles" (p. 134), se identifica una lista de aplicaciones que pueden necesitar un perfil para que funcionen de forma segura.

Siga estos pasos para crear un perfil para cada aplicación:

1. Como usuario `Root`, permita que AppArmor cree un esbozo del perfil de la aplicación ejecutando el comando `genprof` *`nombre_programa`*.

   O bien

   Ejecute *YaST → Novell AppArmor → Asistente para añadir perfiles* e indique la vía completa de la aplicación para la que desea crear un perfil.

   Se creará un perfil básico y AppArmor pasará a modo de aprendizaje, lo que significa que registrará cualquier actividad del programa que esté ejecutando, pero sin limitarlo aún.

2. Ejecute todas las acciones posibles con la aplicación para que AppArmor obtenga una imagen clara de sus actividades.

3. Permita que AppArmor analice los archivos de registro generados en el Paso 2 (p. 136). Puede hacerlo pulsando la tecla S en genprof

   O bien

   Haga clic en *Explorar registro del sistema en busca de eventos de AppArmor* en el *Asistente para añadir perfiles* y siga las instrucciones del asistente hasta completar el perfil.

   AppArmor explorará los registros que haya guardado durante la ejecución de la aplicación y le pedirá que defina los derechos de acceso de cada evento registrado. Puede definirlos para cada archivo o utilizar configuraciones globales.

4 Cuando se hayan definido todos los permisos de acceso, el perfil se establecerá en el modo de aplicación. El perfil se aplicará y AppArmor restringirá la aplicación según este perfil recién creado.

   Si ha iniciado genprof para una aplicación que ya tuviera un perfil en el modo de queja, este perfil seguirá en el modo de aprendizaje hasta que salga de este ciclo de adiestramiento. Para obtener más información acerca de cómo cambiar el modo de un perfil, consulte la sección *Modo de aprendizaje o de queja* (Capítulo 3, *Creación de perfiles de Novell AppArmor, Guía de administración de Novell AppArmor 2.0*) y la sección *Modo de aplicación* (Capítulo 3, *Creación de perfiles de Novell AppArmor, Guía de administración de Novell AppArmor 2.0*).

Pruebe los ajustes del perfil efectuando todas las tareas que necesita con la aplicación que acaba de limitar. Por norma general, el programa limitado se ejecutará sin problemas y no será consciente de las actividades de AppArmor. Sin embargo, si nota algún comportamiento anómalo en la aplicación, compruebe los registros del sistema para ver si AppArmor está poniendo demasiadas limitaciones a la aplicación. Encontrará los registros oportunos en `/var/log/messages` o ejecutando el comando `dmesg`.

Si observa algo parecido al siguiente ejemplo, puede indicar que AppArmor está limitando demasiado la aplicación:

```
AppArmor: REJECTING w access to /var/run/nscd/socket (traceroute(2050) profile
/usr/sbin/traceroute active /usr/sbin/traceroute)
```

Para ajustar el perfil, vuelva a ejecutar el *Asistente para añadir perfiles* como se describe anteriormente y permita que analice los mensajes de registro relativos a esta aplicación concreta. Determine los derechos de acceso o las restricciones cuando YaST lo solicite.

SUGERENCIA: Información adicional

Para obtener más información acerca de la creación y modificación de perfiles, consulte el Capítulo *Creación de perfiles de Novell AppArmor (Guía de administración de Novell AppArmor 2.0)*.

Configuración de notificaciones de eventos e informes de Novell AppArmor

Configure las notificaciones de eventos en Novell AppArmor para poder revisar los eventos de seguridad. La notificación de eventos es una función de Novell AppArmor que informa a un destinatario concreto por correo electrónico cuando se produce una actividad sistemática de Novell AppArmor con el nivel de gravedad seleccionado. Esta función está disponible actualmente a través de la interfaz de YaST.

Para configurar las notificaciones de eventos en YaST, siga estos pasos:

1. Asegúrese de que hay un servidor de correo ejecutándose en el sistema para enviar las notificaciones de eventos.

2. Inicie la sesión como usuario `Root` y abra YaST. A continuación, seleccione *Novell AppArmor → Panel de control de AppArmor.*

3. En la sección *Habilitar notificación de eventos de seguridad,* seleccione *Configurar.*

4. Defina una frecuencia para cada tipo de informe (*Notificación simple, Notificación de resumen* y *Notificación detallada*), introduzca la dirección de correo electrónico que recibirá los informes y determine la gravedad de los eventos que se deben registrar. Si desea incluir eventos de gravedad desconocida en los informes, marque la casilla *Incluir los eventos de gravedad desconocida.*

   NOTA

   A no ser que esté familiarizado con las categorías de eventos de AppArmor, elija la opción para que se le notifiquen los eventos de todos los niveles de gravedad.

5. Salga de este cuadro de diálogo haciendo clic en *Aceptar → Finalizar* para aplicar los ajustes.

Configure informes de Novell AppArmor. Mediante el uso de informes, es posible leer información importante sobre los eventos de seguridad de Novell AppArmor incluida en los archivos de registro sin tener que escudriñar manualmente en la maraña de mensajes que sólo resultan de utilidad para la herramienta logprof. Se puede reducir el tamaño del informe filtrando por periodo de tiempo o por nombre de programa.

Para configurar los informes de AppArmor, siga este procedimiento:

1. Inicie la sesión como usuario `Root` y abra YaST. Seleccione *Novell AppArmor → Informes de AppArmor.*

2. Seleccione el tipo de informe que desee examinar o configurar: *Resumen ejecutivo de seguridad, Auditoría de aplicaciones* o *Informe de incidentes de seguridad.*

3. Modifique la frecuencia de generación de informes, la dirección de correo electrónico, el formato de exportación y la ubicación de los informes haciendo clic en *Editar* e introduciendo los datos necesarios.

4. Para ejecutar un informe del tipo seleccionado, haga clic en *Ejecutar ahora.*

5. Puede desplazarse por los informes archivados de un tipo concreto haciendo clic en *Ver archivo* e indicando el tipo de informe.

   O bien

   Suprima los informes que no necesite o añada otros nuevos.

SUGERENCIA: Información adicional

Para obtener más información acerca de la configuración de las notificaciones de eventos en Novell AppArmor, consulte la sección "Establecimiento de notificaciones de eventos" (Capítulo 4, *Gestión de aplicaciones con perfiles, Guía de administración de Novell AppArmor 2.0*). Para obtener más información acerca de la configuración de los informes, consulte la sección "Informes" (Capítulo 4, *Gestión de aplicaciones con perfiles*, *Guía de administración de Novell AppArmor 2.0*).

Actualización de los perfiles

El software y la configuración del sistema cambian con el tiempo. Como resultado, puede que sea preciso ajustar la configuración de los perfiles de AppArmor de cuando en cuando. AppArmor comprueba el registro del sistema para detectar violaciones de directivas u otros eventos de AppArmor y le permite ajustar el conjunto de perfiles en consecuencia. También se puede tratar cualquier comportamiento de una aplicación que quede fuera de lo definido en el perfil utilizando el *Asistente para actualizar perfiles.*

Para actualizar el conjunto de perfiles, siga este procedimiento:

1. Inicie la sesión como usuario `Root` y abra YaST.
2. Inicie *Novell AppArmor → Asistente para actualizar perfiles.*
3. Cuando se le solicite, ajuste los derechos de acceso o ejecución de cualquier recurso o archivo ejecutable que se haya registrado.
4. Salga de YaST tras contestar a todas las preguntas. Los cambios se aplicarán al perfil oportuno.

SUGERENCIA: Información adicional

Para obtener más información sobre la actualización de los perfiles a partir de los registros del sistema, consulte la sección "Actualización de perfiles a partir de entradas de registro del sistema" (Capítulo 3, *Creación de perfiles de Novell AppArmor, Guía de administración de Novell AppArmor 2.0*).

4.5 Seguridad y confidencialidad

Una de las características principales de un sistema Linux o UNIX es su capacidad de gestionar varios usuarios a la vez (multiusuario) y para permitir que éstos realicen varias tareas (multitarea) en el mismo equipo de forma simultánea. Además, el sistema operativo es transparente para los usuarios. A menudo, los usuarios no saben si los datos y las aplicaciones que utilizan se proporcionan localmente desde su máquina o si su disponibilidad procede de algún otro punto de la red.

Con la capacidad multiusuario, los datos de usuarios distintos deben almacenarse de forma separada. La seguridad y la privacidad deben quedar garantizada. La seguridad de los datos era ya una cuestión importante, aun antes de que los equipos pudieran conectarse a través de redes. Exactamente igual que hoy, la preocupación más importante era la capacidad de mantener la disponibilidad de los datos pese a la pérdida del medio de datos (un disco duro en la mayor parte de los casos) o a otro tipo de daños.

Fundamentalmente, esta sección se centra en problemas de confidencialidad y en los modos de protección de la privacidad de los usuarios; no obstante, nunca se subrayará suficientemente la vital importancia que tienen, para lograr un estado de seguridad

exhaustivo, los procedimientos de creación de copias de seguridad flexibles, puestas a prueba y actualizadas con regularidad. En su defecto, la recuperación de los datos podría ser dificilísima, y no sólo en el caso de algún defecto del hardware, sino también si se sospecha que alguien ha conseguido un acceso no autorizado a los archivos y los ha modificado.

4.5.1 Seguridad local y de red

Hay varias formas de acceder a los datos:

- la comunicación con personas que disponen de la información deseada o del acceso a los datos en un equipo;
- directamente desde la consola de un equipo (acceso físico);
- a través de una línea serie;
- mediante un vínculo de red.

En todos estos casos, el usuario debería autentificarse antes de acceder a los recursos o datos en cuestión. Es posible que un servidor Web sea menos restrictivo a este respecto, pero aun así el usuario no deseará que cualquier internauta pueda acceder a sus datos.

El primero de los casos que figura en la lista anterior es el que implica una mayor dosis de interacción humana; por ejemplo, la solicitud, por parte de un miembro del personal de un banco, de que una persona demuestre ser la propietaria de una cuenta bancaria concreta. En tal caso, se le pide una firma, un PIN o una contraseña que sirvan para constatar su identidad. En algunos casos, es posible obtener ciertos datos de alguien que disponga de determinada información con sólo mencionar retazos y fragmentos para ganar su confianza mediante una retórica brillante. Puede persuadirse a la víctima para que revele, de forma gradual y quizás sin ser consciente de ello, más información. Entre los piratas informáticos (hackers), esto se conoce como *ingeniería social* (social engineering). La educación, así como el tratamiento sensato del lenguaje y la información, constituyen la única protección posible contra estos hechos. Antes de irrumpir en un sistema informático, a menudo los intrusos intentan utilizar a recepcionistas, al personal del servicio técnico o incluso a familiares. En numerosos casos, estos ataques basados en la ingeniería social se descubren pasado mucho tiempo.

Alguien con intenciones de obtener un acceso no autorizado a los datos de un usuario también puede optar por el método tradicional de hacerse directamente con el hardware.

Por lo tanto, la máquina debería protegerse contra cualquier tipo de manipulación para que nadie pueda retirar, sustituir o inutilizar ninguno de sus componentes. Esto se aplica igualmente a las copias de seguridad e incluso a cualquier cable de red o de corriente. También ha de garantizarse la seguridad del procedimiento de arranque, puesto que hay algunas combinaciones de teclas bien conocidas que pueden provocar un comportamiento poco habitual. Evite esto último definiendo contraseñas para el BIOS y el cargador de arranque.

Los terminales en serie conectados a puertos de serie siguen utilizándose en muchos sitios. De forma contraria a las interfaces de red, no se sirven de un protocolo de red para comunicarse con el host. Se hace uso de un simple cable o un puerto de infrarrojos para enviar, en una y otra dirección, caracteres sin formato entre los dispositivos. El propio cable es el punto más débil de un sistema como éste. Resulta fácil grabar cualquier dato que circule por los cables de este sistema con sólo conectar una vieja impresora. Lo que se logra con una impresora también puede llevarse a cabo por otros medios; todo depende del esfuerzo que se invierta en el plan de ataque.

La lectura local de un archivo en un host requiere reglas de acceso diferentes a la de abrir una conexión de red con un servidor en un host distinto. Existe una diferencia entre la seguridad local y la seguridad de red. El límite entre ambos términos radica en la colocación de los datos en paquetes para efectuar su envío.

Seguridad local

La seguridad local comienza con el entorno físico de la ubicación en la que el equipo se encuentra funcionando. Coloque su máquina en un lugar en el que la seguridad esté en consonancia con sus expectativas y necesidades. El objetivo principal de la seguridad local es la de mantener a los usuarios separados unos de otros, de modo que ninguno de ellos pueda hacerse con los permisos o adoptar la identidad de otros. Esta es una regla de aplicación general, aunque adquiere un peso especial con respecto al usuario `root`, que es el que ostenta el poder principal en el sistema. `root` puede adoptar la identidad de cualquier otro usuario local sin que se le solicite ninguna contraseña y, de este modo, leer cualquier archivo almacenado localmente.

Contraseñas

En un sistema Linux, las contraseñas no se almacenan como texto sin formato, ni se espera simplemente a que la cadena de texto introducida coincida con el patrón guardado. Si así fuera, todas las cuentas del sistema se verían en peligro si alguien tuviera acceso

al archivo correspondiente. En lugar de esto, la contraseña almacenada está cifrada y, cada vez que se escribe, se vuelve a cifrar y se efectúa una comparación de ambas cadenas cifradas. Esto sólo proporciona más seguridad si la contraseña cifrada no puede convertirse, mediante ingeniería inversa, en la cadena de texto original.

Esto se consigue de hecho mediante un tipo especial de algoritmo, denominado *trapdoor algorithm* (algoritmo trampilla), puesto que sólo funciona en una dirección. Un intruso que haya logrado hacerse con la cadena cifrada no será capaz de obtener la contraseña con sólo aplicar el mismo algoritmo una vez más. En lugar de eso, necesitaría examinar todas las combinaciones posibles de caracteres hasta hallar la que se pareciera a la contraseña al cifrarse. Con contraseñas de ocho caracteres de longitud, debe calcularse un número considerable de combinaciones posibles.

En la década de los setenta, se argüía que este método aportaría una mayor seguridad que los demás a causa de la relativa lentitud del algoritmo utilizado, que tardaba unos pocos segundos en cifrar una sola contraseña. No obstante, entre tanto, los equipos se han hecho lo suficientemente potentes para efectuar varios cientos de miles o incluso millones de cifrados por segundo. Por ello, las contraseñas cifradas no deberían resultar visibles para los usuarios normales (éstos no pueden leer `/etc/shadow`). Aun más importante resulta que las contraseñas no sean fáciles de adivinar, por si el archivo de contraseña se hace visible a causa de algún error. En consecuencia, no es muy útil "traducir" una contraseña como "tentar" como algo parecido a "t@n1@3".

La sustitución de algunas letras de una palabra por números de apariencia similar no resulta lo suficientemente segura. Los programas de falsificación de contraseñas que utilizan diccionarios para adivinar palabras también funcionan mediante sustituciones de este tipo. Una mejor forma de enmascarar una palabra con un significado poco común, algo que tan sólo tenga sentido para el usuario, como las primeras letras de las palabras de una frase o del título de un libro, como "El nombre de la rosa" de Umberto Eco. Esto daría lugar a la siguiente contraseña segura: "TNotRbUE9". A diferencia de esta última, cualquiera que conozca mínimamente al usuario podría adivinar contraseñas como "cervecero" o "natalia76".

Procedimiento de arranque

Configure su sistema de modo que no pueda arrancarse desde un disquete o CD, bien desmonte por completo las unidades o establezca una contraseña para el BIOS y configure este último para permitir el arranque únicamente desde el disco duro. Un sistema Linux se inicia, por lo general, gracias a un cargador de arranque, lo que permite al usuario transferir opciones adicionales al núcleo arrancado. Evite que otros utilicen

estos parámetros durante el arranque estableciendo una contraseña adicional en `/boot/grub/menu.lst` (consulte el Capítulo 9, *Cargador de arranque* (p. 211)). Éste es un aspecto clave para la seguridad de su sistema. Los permisos `root` hacen posible no sólo la ejecución del propio núcleo, sino que también constituyen la primera autoridad para conceder permisos `root` cuando se inicia el sistema.

Permisos de archivo

Como regla general, se debe trabajar en una tarea dada con los privilegios más restringidos posibles. Por ejemplo, no es en absoluto necesario ser `root` para leer o escribir correo electrónico. Si el programa de correo tiene un error, éste podría aprovecharse en un ataque para el que se necesitasen exactamente los permisos de ese programa cuando se inició. La observancia de la regla anterior minimiza los posibles daños.

Los permisos de los más de 200.000 archivos que se incluyen en una distribución SUSE se seleccionan cuidadosamente. Un administrador del sistema que instale software adicional u otros archivos debería tener un cuidado extremo al actuar así, en especial al establecer los permisos. Un administrador del sistema experimentado y consciente de la importancia de la seguridad siempre utiliza la opción `-l` con el comando `ls` para conseguir una amplia lista de archivos, lo que le permite detectar inmediatamente cualquier incorrección de los permisos de archivos. Un atributo de archivo incorrecto no sólo implica la posibilidad de modificar o borrar los archivos. `root` podría ejecutar estos archivos modificados o, en el caso de archivos de configuración, los programas podrían usarlos con los permisos de `root`. Esto incrementa de forma notable las posibilidades de acción de los intrusos. Los intrusos como los descritos se conocen como "huevos de cuco", puesto que un usuario diferente (que haría las veces de ave) ejecuta el programa (que sería el huevo) como un pájaro cuco que hace que otras aves incuben sus huevos.

El sistema SUSE Linux incluye los archivos `permissions`, `permissions.easy`, `permissions.secure` y `permissions.paranoid`, todos ellos en el directorio `/etc`. El objetivo de estos archivos es definir permisos especiales, como directorios de escritura universal o, en el caso de archivos, el bit setuser ID (los programas con el bit setuser ID definido no funcionan con los permisos del usuario que los ha ejecutado, sino con los permisos del propietario del archivo que, en la mayor parte de los casos, es `root`). Un administrador puede utilizar el archivo `/etc/permissions.local` para añadir sus propios ajustes.

Para definir qué archivos de los anteriormente mencionados utilizan los programas de configuración de SUSE para establecer los permisos como corresponde, seleccione

Security (Seguridad) en YaST. Para obtener más información acerca de este tema, consulte los comentarios en `/etc/permissions` o la página del manual de `chmod` (`man chmod`).

Desbordamiento de buffers y errores de cadenas de formato

Se debe tener especial cuidado siempre que un programa pueda procesar datos que un usuario pueda modificar, aunque ésta es una cuestión que concierne más al programador de la aplicación que a los usuarios normales. El programador debe asegurarse de que la aplicación interprete los datos correctamente, sin escribirlos en las áreas de memoria que son demasiado pequeñas para almacenarlos. Asimismo, el programa debería transferir los datos de un modo coherente, utilizando las interfaces definidas para ello.

Un *desbordamiento de buffer* puede tener lugar si, al escribir en un buffer de memoria, no se tiene en cuenta su tamaño real. Hay casos en los que los datos (tal y como lo genera el usuario) desbordan el espacio disponible en el buffer. El resultado es que los datos se escriben más allá del área del buffer lo que, en determinadas circunstancias, hace posible que un programa ejecute secuencias de programa influido por el usuario (y no por el programador), en lugar de limitarse a procesar los datos del usuario. Un error de este tipo puede acarrear graves consecuencias, sobre todo si el programa se ejecuta con privilegios especiales (consulte "Permisos de archivo" (p. 144)).

Los *errores de cadenas de formato* funcionan de un modo ligeramente distinto, aunque también en este caso es la entrada del usuario la que puede hacer que el programa tenga un funcionamiento incorrecto. En la mayor parte de los casos, estos errores de programación se aprovechan con programas que se ejecutan con permisos especiales (programas setuid y setgid); esto también significa que tanto los datos como el sistema pueden protegerse de tales errores eliminando de los programas los privilegios de ejecución correspondientes. Una vez más, la mejor solución consiste en aplicar el principio del uso mínimo de privilegios (consulte "Permisos de archivo" (p. 144)).

Puesto que los desbordamientos de buffer y los errores de cadenas de formato son errores relacionados con la gestión de los datos de usuario, no sólo pueden explotarse si se ha dado acceso a una cuenta local. Muchos de los errores de los que se ha informado también pueden explotarse mediante un enlace de red. En consecuencia, los desbordamientos de buffer y los errores de cadenas de formato deberían calificarse como relevantes tanto para la seguridad de local como para la de red.

Virus

En contra de lo que suele decirse, existen virus que se ejecutan en Linux. No obstante, los virus que se conocen se iniciaron por sus autores como *prototipos* para probar que la técnica funcionaba como se esperaba. Hasta el momento, no se ha localizado ninguno de estos virus circulando *en libertad*.

Los virus no pueden sobrevivir ni extenderse sin un huésped que los acoja. En este caso, el huésped sería un programa o un área de almacenamiento importante del sistema, como el registro de arranque principal, que necesita poder escribirse para el código de programa del virus. Debido a sus capacidades de multiusuario, Linux puede restringir el acceso de escritura a determinados archivos, con especial importancia de los archivos del sistema. Por lo tanto, si el usuario lleva a cabo su trabajo habitual con permisos `root`, aumenta la probabilidad de que el sistema quede infectado por un virus. Por contra, si se sigue el principio del uso de los mínimos privilegios posibles mencionado anteriormente, la probabilidad de contagio es escasa.

Independientemente de esto, nunca debería ejecutarse precipitadamente un programa de algún sitio desconocido de Internet. Los paquetes SUSE RPM incluyen una firma criptográfica, en forma de etiqueta digital, que pone de manifiesto el cuidado con el que se elaboraron. Los virus son un indicio típico de que el administrador o el usuario carece de la conciencia necesaria acerca de los asuntos relacionados con la seguridad, con lo que se pone en peligro incluso un sistema que, por su mismo diseño, debería gozar de una seguridad extrema.

No deben confundirse los virus con los gusanos, que pertenecen completamente al mundo de las redes. Los gusanos no necesitan un huésped para propagarse.

Seguridad de la red

La seguridad de la red es importante para lograr la protección de un ataque que se inicia en el exterior. El procedimiento de inicio de sesión típico, en el que se solicita un nombre de usuario y una contraseña para autenticar al usuario, constituye un problema del ámbito de la seguridad local. En el caso particular de un inicio de sesión en red, hay que diferenciar dos aspectos relacionados con la seguridad. Lo que tiene lugar hasta que se lleva a cabo la autenticación concierne a la seguridad de red; y todo aquello que ocurre posteriormente incumbe a la seguridad local.

X Window System y X Authentication

Como se mencionó al comienzo, la transparencia de la red es una de las características centrales de un sistema UNIX. X, el sistema de ventanas de los sistemas operativos UNIX, puede utilizar esta función de un modo impresionante. Con X, no existe básicamente ningún problema para iniciar sesión en un host remoto y ejecutar un programa gráfico que, a continuación, se envía a través de la red para mostrarse en el equipo del usuario.

Cuando un cliente X debiera visualizarse de forma remota utilizando un servidor X, éste debería proteger el recurso que gestiona (la visualización) del acceso no autorizado. En términos más concretos, deberían otorgarse ciertos permisos al programa cliente. Con X Window System, hay dos formas de hacer esto, denominados "control del acceso basado en host" y "control de acceso basado en cookies". La primera utiliza la dirección IP del host en el que el cliente debería ejecutarse. El programa que controla esto es xhost. xhost especifica la dirección IP de un cliente legítimo en una minúscula base de datos que pertenece al servidor X. No obstante, el uso de direcciones IP para la autenticación no es muy seguro. Por ejemplo, si hubiera un segundo usuario trabajando en el host y enviando el programa cliente, también tendría acceso al servidor X (como alguien que roba la dirección IP). A causa de estos inconvenientes, este método de autenticación no se describe aquí con mayor detalle, pero puede obtener más información al respecto con `man xhost`.

En el caso del control de acceso basado en cookies, se genera una cadena de caracteres que sólo conoce el servidor X y el usuario legítimo, como un carnet de identidad de algún tipo. Esta cookie (la palabra no hace referencia a las cookies habituales, sino a las galletas ["cookies", en inglés] de la fortuna chinas, que contienen un epigrama) se almacena al iniciar sesión en el archivo `.Xauthority` en el directorio personal del usuario y está disponible para cualquier cliente X que desee utilizar el servidor X para visualizar una ventana. El usuario puede examinar el archivo `.Xauthority` mediante la herramienta xauth. Si se tuviera que cambiar el nombre de `.Xauthority` o si se hubiera suprimido por accidente el archivo del directorio personal, el usuario no sería capaz de abrir ninguna nueva ventana o clientes X. Puede leer más acerca de los mecanismos de seguridad de X Window System en la página Man de Xsecurity (`man Xsecurity`).

Se puede utilizar SSH (shell seguro) para cifrar completamente una conexión de red y reenviarla de forma transparente sin que el usuario perciba el mecanismo de cifrado. Esto también se conoce como "redireccionamiento X" (X forwarding). El redireccionamiento X se logra simulando un servidor X en el lado del servidor y estableciendo una

variable DISPLAY para la shell en el host remoto. Se puede encontrar más información sobre SSH en la Sección 4.2, “SSH: operaciones de red seguras” (p. 121).

AVISO

Si el host en el que se inicia la sesión no se considera seguro, no se debe utilizar el redireccionamiento X. Si el redireccionamiento X está habilitado, un intruso podría autenticarse mediante la conexión SSH para irrumpir en el servidor X y espiar, por ejemplo, las cadenas que se escriben mediante el teclado.

Desbordamiento de buffers y errores de cadenas de formato

Como se indicó en “Desbordamiento de buffers y errores de cadenas de formato” (p. 145), los desbordamientos de buffer y los errores de cadenas de formato deberían calificarse como asuntos relevantes tanto para la seguridad de local como para la de red. Como ocurre con las variantes locales de tales errores, los desbordamientos de buffer en los programas de red se utilizan la mayoría de las veces, cuando se aprovechan convenientemente, para obtener permisos `root`. Aun si no es así, un intruso podría utilizar el error para lograr acceder a una cuenta local sin privilegios para explotar otros puntos débiles que pudiera haber en el sistema.

Los desbordamientos de buffer y los errores de cadenas de formato que pueden explotarse por medio de un enlace de red son, con diferencia, los tipos de ataque más frecuentes en general. Los exploits (programas que se aprovechan de estos fallos de seguridad recién descubiertos) se colocan a menudo en las listas de correo de seguridad. Pueden utilizarse para sacar provecho de la vulnerabilidad sin necesidad de conocer los detalles del código. A lo largo de los años, la experiencia ha demostrado que la disponibilidad de los códigos de los exploits ha contribuido a reforzar la seguridad de los sistemas operativos; esto se debe, obviamente, al hecho de que los desarrolladores de los sistemas operativos se han visto forzados a solucionar el problema que su software presentaba. Con el software libre, cualquiera tiene acceso al código fuente (SUSE Linux viene con todos los códigos fuente disponibles) y aquel que detecte un fallo de seguridad y el código del exploit puede hacer pública la revisión para solucionar el error correspondiente.

Denegación de servicio

El propósito de un ataque DoS (Denegación de servicio) es bloquear un programa del servidor o incluso un sistema al completo, lo que podría lograrse por varios medios: sobrecargando el servidor, manteniéndolo ocupado con paquetes inservibles o explotando un desbordamiento de buffer remoto. A menudo, un ataque DoS se lleva a cabo con el único propósito de hacer que el servicio desaparezca. No obstante, una vez que un servicio dado deja de estar disponible, las comunicaciones pueden volverse vulnerables a los ataques *man-in-the-middle* (sniffing, secuestro de conexión TCP, spoofing) y al envenenamiento de DNS.

Ataques man in the middle: sniffing, secuestro, spoofing

En general, cualquier ataque remoto efectuado por un intruso que se coloca a sí mismo entre los hosts de comunicación se denomina *ataque man-in-the-middle attack*. Lo que casi todos los tipos de ataques man-in-the-middle tienen en común es que la víctima, por lo general, no es consciente de que está ocurriendo algo. Hay muchas variantes posibles; por ejemplo, el intruso puede hacerse con una petición de conexión y redireccionarla a la máquina de destino. En ese momento, la víctima establece, sin darse cuenta, una conexión con el host incorrecto, puesto que el otro extremo se hace pasar por la máquina de destino legítima.

La forma más simple de ataque man-in-the-middle se denomina *sniffer* (en los que el intruso "tan sólo" escucha el tránsito del tráfico de la red). En una forma más compleja de ataque, el intruso "man in the middle" puede intentar apoderarse de una conexión ya establecida (secuestro). Para ello, el intruso necesitaría analizar los paquetes durante cierto tiempo para ser capaz de predecir los números de la secuencia TCP que pertenecen a la conexión. Cuando, finalmente, el intruso asume la función del host de destino, las víctimas se percatan del ataque, puesto que les aparece un mensaje de error que indica el fin de la conexión a causa de un error. El hecho de que haya protocolos sin protección contra los secuestros mediante cifrado, que tan sólo lleva a cabo un procedimiento de autenticación simple al establecer la conexión, facilita la acción de los intrusos.

El *spoofing* es un ataque en el que los paquetes se modifican para que incluyan datos de origen falsos (normalmente, la dirección IP). Las formas más activas de ataque se sirven del envío de paquetes falsos; algo que en una máquina Linux puede efectuar tan sólo el superusuario (`root`).

Muchos de los ataques mencionados se llevan a cabo en combinación con una DoS. Si un intruso tiene la oportunidad de hacer que un host caiga repentinamente, aunque sólo sea por poco tiempo, le resultará más fácil efectuar un ataque activo, puesto que, durante un tiempo, el host no será capaz de detenerlo.

Envenenamiento de DNS

En el envenenamiento de DNS, el intruso corrompe la caché de un servidor DNS respondiéndole con paquetes de respuesta de DNS con identidad suplantada (mediante spoofing), con lo que intenta hacer que el servidor envíe determinados datos a una víctima que solicita información a ese servidor. Muchos servidores mantienen una relación de confianza con otros hosts, basada en direcciones IP o nombres de host. El intruso necesita tener una buena comprensión de la estructura real de las relaciones de confianza entre los hosts para hacerse pasar por uno de los hosts fiables. Por lo general, el intruso analiza algunos paquetes recibidos del servidor para conseguir la información necesaria. A menudo, el intruso también necesita dirigir un ataque DoS oportuno al nombre del servidor. Protéjase utilizando conexiones cifradas capaces de verificar la identidad de los hosts con los cuales se realiza la conexión.

Gusanos

Los gusanos se confunden con frecuencia con los virus, pero hay una clara diferencia entre los dos. Al contrario de lo que ocurre con los virus, los gusanos no necesitan infectar un programa huésped para vivir. En lugar de ello, se especializan en propagarse lo más rápidamente posible en las estructuras de red. Los gusanos que aparecieron en el pasado, como Ramen, Lion o Adore, utilizan fallos de seguridad bien conocidos en los programas de los servidores, como bind8 o lprNG. La protección contra los gusanos es relativamente sencilla. Puesto que hay cierto lapso de tiempo entre el descubrimiento de un fallo de seguridad y el momento en el que el gusano ataca al servidor, hay bastante probabilidad de que una versión actualizada del programa afectado por el fallo se encuentre disponible a tiempo. Esto es útil sólo si el administrador instala las actualizaciones de seguridad en los sistemas en cuestión.

4.5.2 Consejos y trucos generales de seguridad

Para llevar a cabo una gestión competente de la seguridad, es importante mantenerse al día de los nuevos desarrollos y la nueva información relativa a los problemas de seguridad más recientes. Una muy buena forma de proteger un sistema contra problemas de todo tipo es adquirir e instalar, tan rápido como sea posible, los paquetes actualizados que recomiendan los comunicados de seguridad. Los comunicados de seguridad de SUSE se publican en una lista de correo a la que es posible suscribirse a través del enlace `http://www.novell.com/linux/security/securitysupport.html`. La lista `suse-security-announce@suse.de` es una fuente de información de primera mano en lo que respecta a los paquetes actualizados e incluye, entre aquellos que contribuyen activamente, a miembros del equipo de seguridad de SUSE.

La lista de correo `suse-security@suse.de` es un buen lugar para discutir cualquier problema de seguridad que resulte de interés. Suscríbase en la misma página Web.

`bugtraq@securityfocus.com` es una de las listas de correo más conocidas en todo el mundo. Se recomienda su lectura, puesto que recibe entre 15 y 20 publicaciones diarias. Puede encontrarse más información en `http://www.securityfocus.com`.

La lista siguiente enumera una serie de reglas que le resultarán útiles a la hora de resolver determinados asuntos de seguridad básicos:

- De acuerdo con la regla que recomienda usar el conjunto más restrictivo posible de permisos, evite realizar sus tareas como `root`. Con ello, se reduce el riesgo de filtraciones de huevos de cuco o virus y se consigue protección contra los propios errores.

- Si es posible, procure utilizar en todo momento conexiones cifradas para trabajar en una máquina remota. La práctica habitual debería ser utilizar `ssh` (shell segura) para sustituir `telnet`, `ftp`, `rsh` y `rlogin`.

- Evite utilizar los métodos de autenticación basados únicamente en las direcciones IP.

- Intente mantener actualizados los paquetes de elementos más importantes relacionados con la red y suscríbase a las listas de correo correspondientes para recibir

comunicados sobre las nuevas versiones de estos programas (bind, sendmail, ssh, etc.). Esto también se aplica al software relevante para la seguridad local.

- Cambie el archivo `/etc/permissions` para optimizar los permisos de los archivos que sean cruciales para la seguridad del sistema. Si elimina el bit setuid de un programa, éste podría ser incapaz, a partir de entonces, de realizar su trabajo de la forma esperada. Por otro lado, tenga en cuenta que, en la mayor parte de los casos, el programa también dejará de constituir un posible riesgo para la seguridad. Lo anterior puede aplicarse de forma similar a los directorios y archivos de escritura universal.

- Inhabilite todos los servicios de red que el servidor no tenga más remedio que utilizar para funcionar correctamente. Con ello, el sistema incrementará su seguridad. Pueden encontrarse los puertos abiertos con el estado de zócalo LISTEN mediante el programa netstat. En cuanto a las opciones, se recomienda utilizar `netstat -ap` o `netstat -anp`. La opción `-p` permite ver qué proceso ocupa un puerto y con qué nombre.

  Compare los resultados obtenidos al utilizar netstat con los de una exploración exhaustiva de puertos efectuada desde el exterior del host. Para ello, un programa excelente es nmap, que además de comprobar los puertos de la máquina del usuario, también saca conclusiones con respecto a los servicios que se encuentran en espera tras ellos. No obstante, la exploración de puertos puede interpretarse como un acto agresivo, así que no la lleve a cabo en un host si no cuenta con la aprobación explícita del administrador. Por último, recuerde que no sólo es importante explorar los puertos TCP, sino también los UDP (opciones `-sS` y `-sU`).

- Para monitorizar la integridad de los archivos del sistema de un modo fiable, utilice el programa AIDE (Entorno de detección de intrusión avanzada), disponible en SUSE Linux. Cifre las bases de datos creadas por AIDE para impedir que alguien las manipule. Además, disponga de una copia de seguridad de esta base de datos fuera de su máquina, almacenada en un medio de datos externo que no se encuentre conectado a aquélla mediante ningún enlace de red.

- Sea cuidadoso al instalar software de terceros. Se conocen casos en los que un pirata informático (hacker) incluyó un troyano en el archivo tar de un paquete de software de seguridad que, afortunadamente, se descubrió a tiempo. Si instala un paquete binario, procure que no haya dudas sobre el sitio Web del que lo descargó.

Los paquetes RPM de SUSE se distribuyen con la firma gpg. La clave que SUSE utiliza para la firma es:

ID:9C800ACA 2000-10-19 SUSE Package Signing Key <build@suse.de>

Key fingerprint = 79C1 79B2 E1C8 20C1 890F 9994 A84E DAE8 9C80 0ACA

El comando `rpm --checksig package.rpm` muestra si el checksum y la firma de un paquete instalado son correctos. Puede encontrar la clave en el primer CD de la distribución y en la mayor parte de los servidores de clave de todo el mundo.

- Revise con regularidad las copias de seguridad de usuario y los archivos de sistema. Tenga en cuenta que si no comprueba si las copias de seguridad funcionan, éstas pueden resultar completamente inútiles.
- Revise los archivos de registro. Siempre que sea posible, escriba un pequeño guión para buscar entradas sospechosas. Hay que reconocer que no se trata precisamente de una tarea trivial. En última instancia, tan sólo el usuario sabe qué entradas son atípicas y cuáles no.
- Utilice `tcp_wrapper` para restringir el acceso a los servicios individuales que se ejecuten en su máquina, con lo que dispondrá de un control explícito sobre las direcciones IP que pueden conectarse a ese servicio. Para obtener más información sobre `tcp_wrapper`, consulte las páginas del manual de tcpd y de hosts_access (`man 8 tcpd`, `man hosts_access`).
- Utilice SuSEfirewall para mejorar la seguridad proporcionada por tcpd (tcp_wrapper).
- Diseñe las medidas de seguridad para que sean repetitivas: un mensaje que se lea dos veces es mejor que ningún mensaje en absoluto.

4.5.3 Uso de la dirección de notificación de la Central de seguridad

Si descubre algún problema relacionado con la seguridad, escriba un mensaje de correo electrónico a `security@suse.de` después de revisar los paquetes actualizados disponibles. Incluya una descripción actualizada del problema y el número de versión

del paquete en cuestión. SUSE intentará enviar una respuesta lo antes posible. Se recomienda cifrar con pgp sus mensajes de correo electrónico. La clave pgp de SUSE es:

```
ID:3D25D3D9 1999-03-06 SUSE Security Team <security@suse.de>
Key fingerprint = 73 5F 2E 99 DF DB 94 C4 8F 5A A3 AE AF 22 F2 D5
```

Esta clave también se encuentra disponible para su descarga en http://www.novell.com/linux/security/securitysupport.html.

5 Listas de control de acceso en Linux

Las ACL (listas de control de acceso) de POSIX se pueden emplear como una ampliación del concepto tradicional de permisos para los objetos de los sistemas de archivos. Con las ACL, los permisos se pueden definir de forma más flexible de lo que se entiende tradicionalmente por el concepto de permiso.

El término *ACL de POSIX* sugiere que se trata de un estándar verdadero de POSIX (*interfaz de sistema operativo portátil*). Los estándares de borrador POSIX 1003.1e y POSIX 1003.2c se han eliminado por diversas razones. En cualquier caso, los ACL que se encuentran en muchos sistemas que pertenecen a la familia UNIX se basan en dichos borradores, mientras que la aplicación de las ACL de los sistemas de archivos, según se describe en el siguiente capítulo, siguen igualmente estos dos estándares. Ambos estándares pueden verse en `http://wt.xpilot.org/publications/posix.1e/`.

5.1 Permisos de archivo tradicionales

Los aspectos básicos de los permisos de archivos de Linux se explican en la Sección “Usuarios y permisos de acceso” (Capítulo 3, *Cómo trabajar con la shell*, ↑Inicio). Algunas funciones avanzadas son el bit setuid, setgid y adhesivo.

5.1.1 El bit setuid

En algunos casos, los permisos de acceso pueden ser demasiado restrictivos. Por tanto, Linux cuenta con ajustes adicionales que permiten el cambio temporal del usuario y la

identidad del grupo actuales para una acción en concreto. Por ejemplo, el programa `passwd` normalmente necesita permisos de usuario Root para acceder a `/etc/passwd`. Este archivo contiene información importante como los directorios personales de los usuarios o los ID de usuario y de grupo. Por tanto, un usuario normal no podría cambiar `passwd`, porque sería demasiado peligroso otorgar a todos los usuarios acceso directo a este archivo. Una solución posible a este problema es el mecanismo *setuid.* setuid (definir ID de usuario) es un atributo de archivo especial que indica al sistema que debe ejecutar los programas marcados con un ID de usuario en concreto. Considere el comando `passwd`:

```
-rwsr-xr-x  1 root shadow 80036 2004-10-02 11:08 /usr/bin/passwd
```

Puede ver que la `s` indica que el bit setuid está definido para el permiso del usuario. Mediante el bit setuid, todos los usuarios que inician el comando `passwd` lo ejecutan como usuario `Root`.

5.1.2 El bit setgid

El bit setuid se aplica a los usuarios. Sin embargo, hay también una propiedad equivalente para grupos: el bit *setgid.* Un programa para el que se ha definido este bit se ejecuta con el ID de grupo con el que se ha guardado, sin importar el usuario que lo inicia. Por tanto, en un directorio con el bit setgid, todos los archivos o subdirectorios recién creados se asignan al grupo al que pertenece el directorio. Considere el directorio de ejemplo siguiente:

```
drwxrws--- 2 tux archive 48 Nov 19 17:12  backup
```

Puede observar que la `s` indica que el bit setgid está definido para el permiso de grupo. El propietario del directorio y los miembros del grupo `archive` pueden acceder a este directorio. Los usuarios que no sean miembros de este grupo se "asignan" al grupo respectivo. El ID de grupo vigente de todos los archivos escritos será `archive`. Por ejemplo, un programa de copia de seguridad que se ejecuta con el ID de grupo `archive` es capaz de acceder a este directorio incluso sin privilegios de usuario Root.

5.1.3 El bit adhesivo

Existe también el *bit adhesivo.* Es distinto si pertenece a un programa o a un directorio ejecutable. Si pertenece a un programa, un archivo marcado de esta forma se carga en la RAM para evitar la necesidad de obtenerlo del disco duro cada vez que se usa. Este

atributo apenas se utiliza porque los discos duros modernos son lo suficientemente rápidos. Si este bit se asigna a un directorio, impide que los usuarios supriman los archivos de otros usuarios. Los ejemplos típicos incluyen los directorios `/tmp` y `/var/tmp`:

```
drwxrwxrwt 2 root root 1160 2002-11-19 17:15 /tmp
```

5.2 Ventajas de las ACL

Tradicionalmente, se definen tres conjuntos de permisos para cada objeto de archivo de un sistema Linux. Dichos conjuntos incluyen los permisos de lectura (`r`), escritura (`w`) y ejecución (`x`) para cada uno de los tres tipos de usuarios: el propietario del archivo, el grupo y otros usuarios. Por lo demás, también es posible definir el bit *definir id de usuario*, el bit *definir id de grupo* y el bit *de permanencia*. Este concepto básico se adecúa a la perfección a la mayoría de los casos prácticos. Sin embargo, para situaciones más complejas o aplicaciones avanzadas, anteriormente los administradores del sistema tenían que hacer uso de una serie de trucos para sortear las limitaciones del concepto tradicional de permiso.

Las ACL se pueden emplear como una extensión del concepto tradicional de permisos para los archivos. Dichas listas permiten la asignación de permisos a usuarios individuales o a grupos, incluso si éstos no se corresponden con el propietario original ni con el grupo propietario. Las listas de control de acceso son una función del núcleo de Linux y en la actualidad son compatibles con ReiserFS, Ext2, Ext3, JFS y XFS. Gracias al empleo de las ACL, es posible desarrollar las situaciones más complicadas sin tener que implantar complejos modelos de permisos en el nivel de la aplicación.

Las ventajas de las ACL son evidentes si desea sustituir un servidor Windows por uno Linux. Algunas de las estaciones de trabajo conectadas pueden continuar ejecutándose en Windows incluso después de la migración. El sistema Linux ofrece servicios de archivos e impresión a los clientes de Windows mediante el empleo de Samba. Dado que Samba es compatible con las listas de control de acceso, los permisos de usuarios se pueden configurar tanto en el servidor Linux como en Windows con una interfaz gráfica de usuario (únicamente con Windows NT y versiones posteriores). Con `winbindd`, que forma parte del conjunto de aplicaciones Samba, también es posible asignar permisos a usuarios que solamente existen en un dominio de Windows y que no disponen de una cuenta en el servidor Linux.

5.3 Definiciones

clase de usuario
: El concepto convencional de permisos de POSIX hace uso de tres *clases* de usuarios para la asignación de permisos en el sistema de archivos: propietario, grupo propietario y otros usuarios. Se pueden definir tres bits de permiso para cada clase de usuario, lo que hace posible dar permiso para leer, (`r`), escribir (`w`) y ejecutar (`x`).

ACL de acceso
: Los permisos de acceso de usuario y de grupo para todos los tipos de objetos de sistemas de archivos (archivos y directorios) se determinan mediante las ACL de acceso.

ACL por defecto
: Las ACL por defecto se pueden aplicar únicamente a los directorios. Dichas listas determinan los permisos que un objeto de un sistema de archivos hereda de su directorio padre cuando se crea.

entrada de ACL
: Cada ACL cuenta con un conjunto de entradas de ACL. Cada entrada de la ACL contiene un tipo, un calificador para el usuario o el grupo al que hace referencia la entrada y un conjunto de permisos. Para algunos tipos de entradas, el calificador del grupo o de los usuarios no está definido.

5.4 Gestión de las ACL

La Tabla 5.1, “Tipos de entrada de ACL” (p. 159) resume los seis tipos posibles de entradas de ACL, cada una de las cuales define los permisos para un usuario o para un grupo de usuarios. La entrada del *propietario* define los permisos del usuario a quien pertenece el archivo o el directorio. La entrada del *grupo propietario* define los permisos del grupo propietario del archivo. El súperusuario puede cambiar el propietario o el grupo propietario mediante los comandos `chown` o `chgrp`, en cuyo caso las entradas de propietario y de grupo propietario hacen referencia al nuevo propietario y al nuevo grupo propietario. Cada entrada *usuario nombrado* define los permisos del usuario que se especifica en el campo del calificador de la entrada. Cada entrada *grupo nombrado* define los permisos del grupo que se especifican en el campo del calificador de la entrada. Únicamente las entradas del usuario nombrado y del grupo nombrado cuentan

con un campo del calificador que no está vacío. La entrada *otros* define los permisos del resto de usuarios.

La entrada *máscara* aumenta los límites de los permisos asignados a las entradas usuario nombrado, grupo nombrado y grupo propietario mediante la definición de qué permisos en dichas entradas son efectivos y cuáles se encuentran en la máscara. Si existen permisos tanto en una de las entradas mencionadas como en la máscara, dichos permisos serán efectivos. Los permisos contenidos únicamente en la máscara o únicamente en la entrada real no son efectivos, en el sentido de que los permisos no se han otorgado. Todos los permisos definidos en las entradas propietario y grupo propietario son siempre efectivos. El ejemplo que aparece en la Tabla 5.2, "Enmascaramiento de permisos de acceso" (p. 160) demuestra este mecanismo.

Son dos las clases básicas de ACL que existen: La ACL *mínima* contiene únicamente las entradas para los tipos propietario, grupo propietario y otros, que corresponden a los bits de permiso convencionales para archivos y directorios. La ACL *extendida* incluye más elementos; debe contener una entrada máscara y puede contener al mismo tiempo distintas entradas de los tipos usuario nombrado y grupo nombrado.

Tabla 5.1 *Tipos de entrada de ACL*

Tipo	Forma de texto
propietario	`user::rwx`
usuario nombrado	`user:name:rwx`
grupo propietario	`group::rwx`
grupo nombrado	`group:name:rwx`
máscara	`mask::rwx`
otros	`other::rwx`

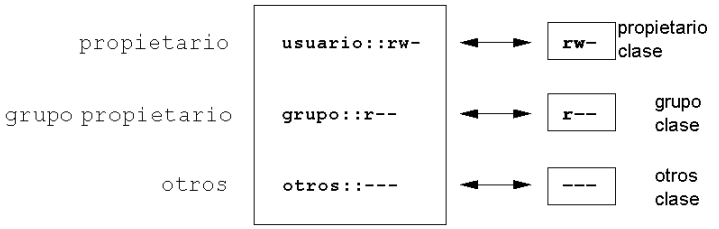
Tabla 5.2 *Enmascaramiento de permisos de acceso*

Tipo de entrada	Forma de texto	Permisos
usuario nombrado	`user:geeko:r-x`	`r-x`
máscara	`mask::rw-`	`rw-`
	permisos efectivos:	`r--`

5.4.1 Entradas ACL y bits de permiso de modos de archivos

Tanto la Figura 5.1, “ACL mínima: entradas ACL comparadas con los bits de permiso” (p. 160) como la Figura 5.2, “ACL extendida: entradas ACL comparadas con los bits de permiso” (p. 161) ilustran dos casos de una ACL mínima y una ACL extendida. Las figuras se estructuran en tres bloques, el primero de los cuales muestra las especificaciones de tipo de las entradas ACL, mientras que en el bloque central aparece un ejemplo de ACL. El bloque situado en el extremo derecho, por su parte, muestra los bits de permiso respectivos de acuerdo con el concepto convencional de permiso, como muestra, por ejemplo, `ls -l`. En ambos casos, los permisos de la *clase de propietario* se asignan a la entrada ACL propietario. Los permisos *otras clases* se asignan a la entrada ACL respectiva. Sin embargo, la asignación de los permisos de la *clase de grupo* es diferente en los dos casos.

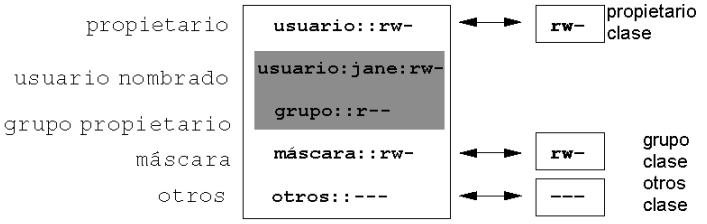
Figura 5.1 *ACL mínima: entradas ACL comparadas con los bits de permiso*



En el caso de una ACL mínima (sin máscara), los permisos de la clase de grupo se asignan al grupo propietario de la entrada ACL. Esta situación se muestra en la Figura 5.1, “ACL mínima: entradas ACL comparadas con los bits de permiso” (p. 160).

En el caso de una ACL extendida (con máscara), los permisos de la clase de grupo se asignan a la entrada de máscara. Esta situación se muestra en la Figura 5.2, “ACL extendida: entradas ACL comparadas con los bits de permiso” (p. 161).

Figura 5.2 *ACL extendida: entradas ACL comparadas con los bits de permiso*



Esta modalidad de asignación asegura una interacción de aplicaciones sin brusquedades, con independencia de si son compatibles con ACL. Los permisos de acceso que se asignaron mediante los bits de permiso representan el límite superior para los “ajustes finos” restantes hechos con una ACL. Los cambios efectuados en los bits de permiso los refleja la ACL y viceversa.

5.4.2 Directorio con una ACL de acceso

Con `getfacl` y `setfacl` en la línea de comandos, se puede acceder a las ACL. La forma en que se utilizan estos comandos se describen en el siguiente ejemplo:

Antes de crear el directorio, utilice el comando `umask` para definir qué permisos de acceso deben enmascararse cada vez que se crea un objeto de archivo. El comando `umask 027` establece los permisos por defecto dando al propietario la gama completa de permisos (`0`), denegando al grupo el acceso de escritura (`2`) y no concediendo a otros usuarios ningún permiso (`7`). En realidad, el comando `umask` enmascara los bits de permiso correspondientes o los desactiva. Para obtener más información, consulte la página Man de `umask`.

El comando `mkdir mydir` crea el directorio `mydir` con los permisos por defecto establecidos por el comando `umask`. Utilice el comando `ls -dl mydir` para comprobar si todos los permisos se han asignado correctamente. Los datos de salida para este ejemplo son:

```
drwxr-x--- ... tux project3 ... mydir
```

Compruebe el estado inicial de la ACL con `getfacl mydir`. La información que se ofrecerá será del tipo:

```
# file: mydir
# owner: tux
# group: project3
user::rwx
group::r-x
other::---
```

Las tres primeras líneas de los datos de salida muestran el nombre, el propietario y el grupo propietario del directorio. Las tres líneas siguientes contienen estas tres entradas ACL: propietario, grupo propietario y otros. De hecho, en el caso de esta ACL mínima, el comando `getfacl` no ofrece ninguna información que no se pueda obtener mediante el comando `ls`.

Modifique la ACL para asignar permisos de lectura, escritura y ejecución a un usuario adicional `geeko` y a un grupo adicional `mascots` con:

```
setfacl -m user:geeko:rwx,group:mascots:rwx mydir
```

La opción `-m` origina que el comando `setfacl` modifique la ACL existente. El siguiente argumento indica las entradas ACL que se van a modificar (las entradas múltiples se separan con comas). La parte final especifica el nombre del directorio al que se deben aplicar estas modificaciones. Utilice el comando `getfacl` para visualizar la ACL resultante.

```
# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx
group::r-x
group:mascots:rwx
mask::rwx
other::---
```

Además de las entradas iniciadas por el usuario `geeko` y el grupo `mascots`, se ha generado una entrada máscara. La entrada máscara mencionada se fija de forma automática de forma tal que todos los permisos sean efectivos. El comando `setfacl` adapta automáticamente las entradas máscara existentes a los ajustes modificados, salvo en el caso de que haya desactivado esta función con `-n`. La entrada máscara define los permisos máximos de acceso efectivos para todas las entradas que se encuentran en la clase de grupo. Se incluyen aquí usuario nombrado, grupo nombrado y grupo propietario. Los bits de permiso de clase de grupo que muestra `ls -dl mydir` corresponden ahora a la entrada `máscara`.

```
drwxrwx---+ ... tux project3 ... mydir
```

La primera columna de los datos de salida contiene un signo + adicional para indicar la existencia de una ACL *extendida* para este elemento.

De acuerdo con los datos de salida del comando `ls`, los permisos para la entrada máscara incluyen el acceso de escritura. Tradicionalmente, tales bits de permiso indicarían que el grupo propietario (en este caso, `proyecto3`) cuenta también con acceso de escritura al directorio `mydir`. Sin embargo, los permisos de acceso efectivo para el grupo propietario se corresponden con la porción coincidente de los permisos definidos por el grupo propietario y por la máscara, que en nuestro ejemplo es `r-x` (consulte la Tabla 5.2, “Enmascaramiento de permisos de acceso” (p. 160)). En lo concerniente a los permisos efectivos del grupo propietario en este ejemplo, no se ha producido ninguna modificación, incluso tras la inclusión de las entradas ACL.

Edite la entrada máscara con los comandos `setfacl` o `chmod`. Por ejemplo, utilice el comando `chmod g-w mydir`. El comando `ls -dl mydir` mostrará a continuación:

```
drwxr-x---+ ... tux project3 ... mydir
```

El comando `getfacl mydir` proporciona los siguientes datos de salida:

```
# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx          # effective: r-x
group::r-x
group:mascots:rwx       # effective: r-x
mask::r-x
other::---
```

Después de ejecutar el comando `chmod` para eliminar el permiso de escritura de los bits de la clase de grupo, los datos de salida del comando `ls` son suficientes para comprobar que los bits de la máscara deben haber cambiado de la forma correspondiente: el permiso de escritura está de nuevo limitado al propietario de `mydir`. Los datos de salida del comando `getfacl` confirman la afirmación anterior. Dichos datos de salida incluyen un comentario para todas aquellas entradas en las que los bits de permiso efectivo no se corresponden con los permisos originales, debido a que se han filtrado de acuerdo con la entrada máscara. Los permisos originales se pueden restaurar en cualquier momento mediante el comando `chmod g+w mydir`.

5.4.3 Directorio con una ACL por defecto

Los directorios pueden tener una ACL, es decir, un tipo especial de ACL que define los permisos de acceso que heredan los objetos del directorio cuando se crean. La ACL por defecto afectará tanto a los subdirectorios como a los archivos.

Efectos de una ACL por defecto

Son dos las maneras mediante las que los permisos de una ACL por defecto de un directorio se transfieren a los archivos y subdirectorios de dicho directorio:

- El subdirectorio hereda la ACL por defecto del directorio padre en calidad tanto de ACL por defecto como de ACL de acceso.
- El archivo hereda la ACL por defecto como ACL de acceso.

Todas las llamadas del sistema que crean objetos de sistemas de archivos utilizan un parámetro `mode` que define los permisos de acceso para el objeto de sistemas de archivos creado recientemente. Si el directorio padre no dispone de una ACL por defecto, los bits de permiso que definió `umask` se sustraen de los permisos al pasar por parámetro `mode`, y el resultado se asigna al nuevo objeto. Si existe una ACL por defecto para el directorio padre, los bits de permiso asignados al nuevo objeto se corresponden con la porción coincidente de los permisos del parámetro `mode` y con aquellos que se definen en la ACL por defecto. El comando `umask` se descarta en este caso.

Aplicación de las ACL por defecto

Los tres ejemplos siguientes muestran las principales operaciones que se pueden aplicar a los directorios y las ACL por defecto:

1. Añada una ACL por defecto al directorio existente `mydir` con:

   ```
   setfacl -d -m group:mascots:r-x mydir
   ```

   La opción `-d` del comando `setfacl` origina que el comando `setfacl` lleve a cabo las siguientes modificaciones (opción `-m`) en la ACL por defecto.

   Compruebe el resultado del siguiente comando:

   ```
   getfacl mydir
   ```

```
# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx
group::r-x
group:mascots:rwx
mask::rwx
other::---
default:user::rwx
default:group::r-x
default:group:mascots:r-x
default:mask::r-x
default:other::---
```

El comando `getfacl` ofrece como resultado tanto la ACL de acceso como la ACL por defecto. La ACL por defecto se compone de todas las líneas que comienzan por `default`. Aunque usted ejecutó solamente el comando `setfacl` con una entrada para el grupo `mascots` para obtener la ACL por defecto, el comando `setfacl` ha copiado automáticamente las entradas restantes de la ACL de acceso para crear una ACL por defecto válida. Las ACL por defecto no tienen un efecto intermedio en los permisos de acceso. Únicamente intervienen cuando se crean los objetos de sistemas de archivos. Estos nuevos objetos solamente heredan permisos de la ACL por defecto de sus directorios padre.

2. En el siguiente ejemplo, utilice el comando `mkdir` para crear un subdirectorio en `mydir`, que heredará la ACL por defecto.

```
mkdir mydir/mysubdir

getfacl mydir/mysubdir

# file: mydir/mysubdir
# owner: tux
# group: project3
user::rwx
group::r-x
group:mascots:r-x
mask::r-x
other::---
default:user::rwx
default:group::r-x
default:group:mascots:r-x
default:mask::r-x
default:other::---
```

Tal y como se preveía, el subdirectorio que se acaba de crear, `mysubdir`, tiene los permisos de la ACL por defecto del directorio padre. La ACL de acceso de

`mysubdir` es una copia exacta de la ACL por defecto de `mydir`. La ACL por defecto que este directorio transmitirá a los objetos dependientes de él será también la misma.

3. Utilice el comando `touch` para crear un archivo en el directorio `mydir`, por ejemplo, `touch mydir/myfile`. El comando `ls -l mydir/myfile` mostrará entonces:

```
-rw-r-----+ ... tux project3 ... mydir/myfile
```

Los datos de salida del comando `getfacl mydir/myfile` son:

```
# file: mydir/myfile
# owner: tux
# group: proyecto3
user::rw-
group::r-x          # effective:r--
group:mascots:r-x   # effective:r--
mask::r--
other::---
```

El comando `touch` utiliza un `mode` con el valor `0666` al crear nuevos archivos, lo que significa que los archivos se crean con permisos de lectura y escritura para todas las clases de usuarios, siempre y cuando no existan restricciones en el comando `umask` ni en la ACL por defecto (consulte "Efectos de una ACL por defecto" (p. 164)). De hecho, esto indica que todos los permisos no contenidos en el valor `mode` se han eliminado de las entradas ACL correspondientes. Aunque no se ha eliminado ningún permiso de la entrada ACL de la clase de grupo, la entrada máscara se ha modificado para enmascarar los permisos no establecidos en el valor `mode`.

Esta medida asegura una interacción sin interrupciones de aplicaciones, tales como compiladores, con las ACL. Puede crear archivos con permisos restringidos de acceso y, posteriormente, marcarlos como ejecutables. El mecanismo `máscara` garantiza que los usuarios y los grupos adecuados puedan ejecutar dichos archivos de la forma deseada.

5.4.4 Algoritmo de comprobación de ACL

Se aplica un algoritmo de comprobación antes de que cualquier proceso o aplicación pueda acceder a un objeto de sistemas de archivos protegido por la ACL. Por norma general, las entradas ACL se examinan de acuerdo con la siguiente secuencia: propie-

tario, usuario nombrado, grupo propietario o grupo nombrado y otros. El acceso se gestiona de acuerdo con la entrada que mejor se adapta al proceso. Los permisos no se acumulan.

La operación, sin embargo, es más complicada si un proceso pertenece a más de un grupo, por lo que podría adaptarse a varias entradas de grupo. Se selecciona una entrada forma aleatoria de entre las entradas adecuadas que cuentan los permisos necesarios. No es relevante cuál de las entradas origina el resultado final "acceso autorizado". Así mismo, si ninguna de las entradas de grupo adecuadas cuenta con los permisos necesarios, una entrada seleccionada de forma aleatoria origina el resultado final "acceso denegado".

5.5 Compatibilidad de ACL con las aplicaciones

Las ACL se pueden emplear para implantar situaciones de permisos de gran complejidad que cumplan los requisitos de las aplicaciones más actuales. El concepto tradicional de permiso y las ACL se pueden combinar de forma inteligente. Tanto las ACL como Samba y Konqueror admiten los comandos básicos de archivos (`cp`, `mv`, `ls`, etc.).

Por desgracia, muchos editores y administradores de archivos no son aún compatibles con ACL. Cuando se copian archivos con Emacs, por ejemplo, las ACL de estos archivos se pierden. Cuando se modifican archivos con un editor, las ACL de los archivos en algunos casos se mantienen y en otros no, dependiendo del modo de copias de seguridad del editor empleado. Si el editor escribe los cambios en el archivo original, se mantiene la ACL de acceso. Si el editor guarda los contenidos actualizados en un archivo nuevo que recibe el nombre del archivo anterior, se pueden perder las ACL, a menos que el editor sea compatible con las ACL. Excepto en el caso de star archiver, no hay en la actualidad aplicaciones de copias de seguridad que conserven las ACL.

5.6 Información adicional

La información detallada sobre las ACL se encuentra disponible en `http://acl.bestbits.at/`. Consulte también las páginas Man para los comandos `getfacl(1)`, `acl(5)` y `setfacl(1)`.

Utilidades de monitorización del sistema

6

Se pueden utilizar varios programas y mecanismos, algunos de los cuales están representados aquí, para examinar el estado del sistema. También se describen algunas utilidades especialmente indicadas para las tareas habituales, junto con los parámetros más importantes.

Para cada uno de los comandos introducidos, se presentan ejemplos de las salidas relevantes. En estos ejemplos, la primera línea es el comando en sí mismo (después del signo > o de la almohadilla). Las omisiones se indican con corchetes (`[...]`) y las líneas largas se acortan cuando es necesario. Los saltos de línea para las líneas largas se indican con una barra invertida (\).

```
# command -x -y
output line 1
output line 2
output line 3 is annoyingly long, so long that \
    we have to break it
output line 3
[...]
output line 98
output line 99
```

Se han hecho descripciones cortas para permitir que se mencionen tantas utilidades como sea posible. El resto de información de todos los comandos se puede encontrar en las páginas Man. La mayoría de comandos también admiten el parámetro `--help`, que produce una lista breve de posibles parámetros.

6.1 Lista de archivos abiertos: `lsof`

Para ver una lista de todos los archivos abiertos para el proceso con el ID de proceso *`PID`*, utilice `-p`. Por ejemplo, para ver todos los archivos utilizados por la shell actual, introduzca:

```
tester@linux:~> lsof -p $$
COMMAND  PID   USER   FD   TYPE DEVICE    SIZE   NODE NAME
bash    5552 tester  cwd    DIR    3,3    1512 117619 /home/tester
bash    5552 tester  rtd    DIR    3,3     584      2 /
bash    5552 tester  txt    REG    3,3  498816  13047 /bin/bash
bash    5552 tester  mem    REG    0,0              0 [heap] (stat: No such
\
 file or directory)
bash    5552 tester  mem    REG    3,3  217016 115687 /var/run/nscd/passwd
bash    5552 tester  mem    REG    3,3  208464  11867 \
 /usr/lib/locale/en_GB.utf8/LC_CTYPE
bash    5552 tester  mem    REG    3,3  882134  11868 \
 /usr/lib/locale/en_GB.utf8/LC_COLLATE
bash    5552 tester  mem    REG    3,3 1386997   8837 /lib/libc-2.3.6.so
bash    5552 tester  mem    REG    3,3   13836   8843 /lib/libdl-2.3.6.so
bash    5552 tester  mem    REG    3,3  290856  12204 /lib/libncurses.so.5.5
bash    5552 tester  mem    REG    3,3   26936  13004 /lib/libhistory.so.5.1
bash    5552 tester  mem    REG    3,3  190200  13006 /lib/libreadline.so.5.1
bash    5552 tester  mem    REG    3,3      54  11842 \
 /usr/lib/locale/en_GB.utf8/LC_NUMERIC
bash    5552 tester  mem    REG    3,3    2375  11663 \
 /usr/lib/locale/en_GB.utf8/LC_TIME
bash    5552 tester  mem    REG    3,3     290  11736 \
 /usr/lib/locale/en_GB.utf8/LC_MONETARY
bash    5552 tester  mem    REG    3,3      52  11831 \
 /usr/lib/locale/en_GB.utf8/LC_MESSAGES/SYS_LC_MESSAGES
bash    5552 tester  mem    REG    3,3      34  11862 \
 /usr/lib/locale/en_GB.utf8/LC_PAPER
bash    5552 tester  mem    REG    3,3      62  11839 \
 /usr/lib/locale/en_GB.utf8/LC_NAME
bash    5552 tester  mem    REG    3,3     127  11664 \
 /usr/lib/locale/en_GB.utf8/LC_ADDRESS
bash    5552 tester  mem    REG    3,3      56  11735 \
 /usr/lib/locale/en_GB.utf8/LC_TELEPHONE
bash    5552 tester  mem    REG    3,3      23  11866 \
 /usr/lib/locale/en_GB.utf8/LC_MEASUREMENT
bash    5552 tester  mem    REG    3,3   21544   9109 \
 /usr/lib/gconv/gconv-modules.cache
bash    5552 tester  mem    REG    3,3     366   9720 \
 /usr/lib/locale/en_GB.utf8/LC_IDENTIFICATION
bash    5552 tester  mem    REG    3,3   97165   8828 /lib/ld-2.3.6.so
bash    5552 tester    0u   CHR  136,5              7 /dev/pts/5
bash    5552 tester    1u   CHR  136,5              7 /dev/pts/5
```

```
bash    5552 tester    2u   CHR  136,5              7 /dev/pts/5
bash    5552 tester  255u   CHR  136,5              7 /dev/pts/5
```

Se ha utilizado la variable de la shell especial $$, cuyo valor es el ID de proceso de la shell.

El comando `lsof` muestra todos los archivos abiertos actualmente si se utilizan sin ningún parámetro. Como suele haber miles de archivos abiertos, mostrarlos todos casi nunca es útil. Sin embargo, la lista de todos los archivos se puede combinar con las funciones de búsqueda para generar listas útiles. Por ejemplo, muestre todos los dispositivos de caracteres utilizados:

```
tester@linux:~> lsof | grep CHR
bash      3838     tester    0u      CHR  136,0                2 /dev/pts/0
bash      3838     tester    1u      CHR  136,0                2 /dev/pts/0
bash      3838     tester    2u      CHR  136,0                2 /dev/pts/0
bash      3838     tester  255u      CHR  136,0                2 /dev/pts/0
bash      5552     tester    0u      CHR  136,5                7 /dev/pts/5
bash      5552     tester    1u      CHR  136,5                7 /dev/pts/5
bash      5552     tester    2u      CHR  136,5                7 /dev/pts/5
bash      5552     tester  255u      CHR  136,5                7 /dev/pts/5
X         5646       root  mem       CHR    1,1             1006 /dev/mem
lsof      5673     tester    0u      CHR  136,5                7 /dev/pts/5
lsof      5673     tester    2u      CHR  136,5                7 /dev/pts/5
grep      5674     tester    1u      CHR  136,5                7 /dev/pts/5
grep      5674     tester    2u      CHR  136,5                7 /dev/pts/5
```

6.2 Usuarios que acceden a los archivos: `fuser`

Puede que sea útil determinar qué procesos o usuarios están accediendo actualmente a ciertos archivos. Supongamos, por ejemplo, que desea desmontar un sistema de archivos montado en `/mnt`. `umount` devuelve el mensaje "device is busy" (el dispositivo está ocupado). A continuación, se puede utilizar el comando `fuser` para determinar qué procesos acceden al dispositivo:

```
tester@linux:~> fuser -v /mnt/*

                     USER        PID ACCESS COMMAND
/mnt/notes.txt       tester    26597 f....  less
```

Una vez terminado el proceso `less`, que se estaba ejecutando en otra terminal, el sistema de archivos se puede desmontar de forma correcta.

6.3 Propiedades del archivo: stat

El comando stat muestra las propiedades del archivo:

```
tester@linux:~> stat /etc/profile
  File: `/etc/profile'
  Size: 7930            Blocks: 16         IO Block: 4096   regular file
Device: 303h/771d       Inode: 40657       Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2006-01-06 16:45:43.000000000 +0100
Modify: 2005-11-21 14:54:35.000000000 +0100
Change: 2005-12-19 09:51:04.000000000 +0100
```

El parámetro --filesystem genera información detallada de las propiedades del sistema de archivos en el que se ubica el archivo especificado:

```
tester@linux:~> stat /etc/profile --filesystem
  File: "/etc/profile"
    ID: 0        Namelen: 255     Type: reiserfs
Block size: 4096       Fundamental block size: 4096
Blocks: Total: 2622526    Free: 1809771    Available: 1809771
Inodes: Total: 0          Free: 0
```

6.4 Dispositivos USB: lsusb

El comando lsusb muestra todos los dispositivos USB. Con la opción -v, imprima una lista más detallada. La información detallada se lee en el directorio /proc/bus/usb/. A continuación se muestra la salida del comando lsusb con los siguientes dispositivos USB interconectados: nodo central, tarjeta memory stick, disco duro y un ratón.

```
linux:/ # lsusb
Bus 004 Device 007: ID 0ea0:2168 Ours Technology, Inc. Transcend JetFlash \
 2.0 / Astone USB Drive
Bus 004 Device 006: ID 04b4:6830 Cypress Semiconductor Corp. USB-2.0 IDE \
 Adapter
Bus 004 Device 005: ID 05e3:0605 Genesys Logic, Inc.
Bus 004 Device 001: ID 0000:0000
Bus 003 Device 001: ID 0000:0000
Bus 002 Device 001: ID 0000:0000
Bus 001 Device 005: ID 046d:c012 Logitech, Inc. Optical Mouse
Bus 001 Device 001: ID 0000:0000
```

6.5 Información acerca de un dispositivo SCSI: `scsiinfo`

El comando `scsiinfo` muestra información acerca de un dispositivo SCSI. Con la opción `-l`, muestre todos los dispositivos SCSI que el sistema conoce (con el comando `lsscsi` se obtiene información similar). La siguiente es la salida de `scsiinfo -i /dev/sda`, que proporciona información acerca de un disco duro. La opción `-a` proporciona incluso más información.

```
linux:/ # scsiinfo -i /dev/sda
Inquiry command
---------------
Relative Address                  0
Wide bus 32                       0
Wide bus 16                       1
Synchronous neg.                  1
Linked Commands                   1
Command Queueing                  1
SftRe                             0
Device Type                       0
Peripheral Qualifier              0
Removable?                        0
Device Type Modifier              0
ISO Version                       0
ECMA Version                      0
ANSI Version                      3
AENC                              0
TrmIOP                            0
Response Data Format              2
Vendor:                   FUJITSU
Product:                  MAS3367NP
Revision level:           0104A0K7P43002BE
```

La opción `-d` extrae una lista de deficiencias con dos tablas de bloques incorrectos de un disco duro: en primer lugar, la proporcionada por el proveedor (tabla del fabricante) y en segundo lugar, la lista de bloques incorrectos que aparecieron en la operación (tabla generada). Si aumenta el número de entradas de la tabla generada, puede que sea una buena idea sustituir el disco duro.

6.6 Procesos: `top`

El comando `top`, que significa "tabla de procesos", muestra una lista de procesos que se actualiza cada dos segundos. Para salir del programa, pulse Q. El parámetro `-n`

`1` termina el programa después de mostrar una vez la lista de procesos. A continuación, se ofrece un ejemplo de salida del comando `top -n 1`:

```
tester@linux:~> top -n 1
top - 17:06:28 up  2:10,  5 users,  load average: 0.00, 0.00, 0.00
Tasks:  85 total,   1 running,  83 sleeping,   1 stopped,   0 zombie
Cpu(s):  5.5% us,  0.8% sy,  0.8% ni, 91.9% id,  1.0% wa,  0.0% hi,  0.0% si
Mem:    515584k total,   506468k used,     9116k free,    66324k buffers
Swap:   658656k total,        0k used,   658656k free,   353328k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
    1 root      16   0   700  272  236 S  0.0  0.1   0:01.33 init
    2 root      34  19     0    0    0 S  0.0  0.0   0:00.00 ksoftirqd/0
    3 root      10  -5     0    0    0 S  0.0  0.0   0:00.27 events/0
    4 root      10  -5     0    0    0 S  0.0  0.0   0:00.01 khelper
    5 root      10  -5     0    0    0 S  0.0  0.0   0:00.00 kthread
   11 root      10  -5     0    0    0 S  0.0  0.0   0:00.05 kblockd/0
   12 root      20  -5     0    0    0 S  0.0  0.0   0:00.00 kacpid
  472 root      20   0     0    0    0 S  0.0  0.0   0:00.00 pdflush
  473 root      15   0     0    0    0 S  0.0  0.0   0:00.06 pdflush
  475 root      11  -5     0    0    0 S  0.0  0.0   0:00.00 aio/0
  474 root      15   0     0    0    0 S  0.0  0.0   0:00.07 kswapd0
  681 root      10  -5     0    0    0 S  0.0  0.0   0:00.01 kseriod
  839 root      10  -5     0    0    0 S  0.0  0.0   0:00.02 reiserfs/0
  923 root      13  -4  1712  552  344 S  0.0  0.1   0:00.67 udevd
 1343 root      10  -5     0    0    0 S  0.0  0.0   0:00.00 khubd
 1587 root      20   0     0    0    0 S  0.0  0.0   0:00.00 shpchpd_event
 1746 root      15   0     0    0    0 S  0.0  0.0   0:00.00 w1_control
 1752 root      15   0     0    0    0 S  0.0  0.0   0:00.00 w1_bus_master1
 2151 root      16   0  1464  496  416 S  0.0  0.1   0:00.00 acpid
 2165 messageb  16   0  3340 1048  792 S  0.0  0.2   0:00.64 dbus-daemon
 2166 root      15   0  1840  752  556 S  0.0  0.1   0:00.01 syslog-ng
 2171 root      16   0  1600  516  320 S  0.0  0.1   0:00.00 klogd
 2235 root      15   0  1736  800  652 S  0.0  0.2   0:00.10 resmgrd
 2289 root      16   0  4192 2852 1444 S  0.0  0.6   0:02.05 hald
 2403 root      23   0  1756  600  524 S  0.0  0.1   0:00.00 hald-addon-acpi
 2709 root      19   0  2668 1076  944 S  0.0  0.2   0:00.00 NetworkManagerD
 2714 root      16   0  1756  648  564 S  0.0  0.1   0:00.56 hald-addon-stor
```

Si pulsa F mientras se ejecuta `top`, se abre un menú con el que realizar cambios significativos al formato de la salida.

El parámetro `-U` *`UID`* monitoriza sólo los procesos asociados con un usuario en concreto. Sustituya *`UID`* por el ID del usuario. El comando `top -U` `` `id -u` `` devuelve el UID del usuario dependiendo del nombre de usuario y muestra sus procesos.

6.7 Lista de procesos: ps

El comando `ps` produce una lista de procesos. La mayoría de parámetros deben escribirse sin un signo menos. Con el comando `ps --help` podrá acceder a información general, o bien, consulte la página Man para obtener información más detallada.

Para mostrar todos los procesos con la información del usuario y de la línea de comandos, utilice el comando `ps axu`:

```
tester@linux:~> ps axu
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0    696   272 ?        S    12:59   0:01 init [5]
root         2  0.0  0.0      0     0 ?        SN   12:59   0:00 [ksoftirqd/0]
root         3  0.0  0.0      0     0 ?        S<   12:59   0:00 [events/0]
[...]
tester    4047  0.0  6.0 158548 31400 ?        Ssl  13:02   0:06 mono-best \
 --debug /usr/lib/beagle/Best.exe --autostarted
tester    4057  0.0  0.7   9036  3684 ?        Sl   13:02   0:00 \
 /opt/gnome/sbin/gnome-vfs-daemon
--oaf-activate-iid=OAFIID:GNOME_VFS_Daemon_Factory --oa
tester    4067  0.0  0.1   2204   636 ?        S    13:02   0:00 \
 /opt/gnome/lib/nautilus/mapping-daemon
tester    4072  0.0  1.0  15996  5160 ?        Ss   13:02   0:00 \
 gnome-screensaver
tester    4114  0.0  3.7 130988 19172 ?        SLl  13:06   0:04 sound-juicer
tester    4818  0.0  0.3   4192  1812 pts/0    Ss   15:59   0:00 -bash
tester    4959  0.0  0.1   2324   816 pts/0    R+   16:17   0:00 ps axu
```

Para comprobar cuántos procesos `sshd` se están ejecutando, utilice la opción `-p` junto con el comando `pidof`, que servirá para mostrar los ID de los procesos dados.

```
tester@linux:~> ps -p `pidof sshd`
  PID TTY      STAT   TIME COMMAND
 3524 ?        Ss     0:00 /usr/sbin/sshd -o PidFile=/var/run/sshd.init.pid
 4813 ?        Ss     0:00 sshd: tester [priv]
 4817 ?        R      0:00 sshd: tester@pts/0
```

La lista de procesos se puede formatear de acuerdo con las necesidades de cada uno. La opción `-L` devuelve una lista de todas las palabras clave. Introduzca el siguiente comando para generar una lista de todos los procesos clasificados según la utilización de la memoria:

```
tester@linux:~> ps ax --format pid,rss,cmd --sort rss
  PID   RSS CMD
    2     0 [ksoftirqd/0]
    3     0 [events/0]
    4     0 [khelper]
    5     0 [kthread]
```

```
   11     0 [kblockd/0]
   12     0 [kacpid]
  472     0 [pdflush]
  473     0 [pdflush]
[...]
 4028 17556 nautilus --no-default-window --sm-client-id default2
 4118 17800 ksnapshot
 4114 19172 sound-juicer
 4023 25144 gnome-panel --sm-client-id default1
 4047 31400 mono-best --debug /usr/lib/beagle/Best.exe --autostarted
 3973 31520 mono-beagled --debug /usr/lib/beagle/BeagleDaemon.exe \
  --bg --autostarted
```

6.8 Árbol de procesos: `pstree`

El comando `pstree` produce una lista de procesos en forma de árbol:

```
tester@linux:~> pstree
init-+-NetworkManagerD
     |-acpid
     |-3*[automount]
     |-cron
     |-cupsd
     |-2*[dbus-daemon]
     |-dbus-launch
     |-dcopserver
     |-dhcpcd
     |-events/0
     |-gpg-agent
     |-hald-+-hald-addon-acpi
     |      `-hald-addon-stor
     |-kded
     |-kdeinit-+-kdesu---su---kdesu_stub---yast2---y2controlcenter
     |         |-kio_file
     |         |-klauncher
     |         |-konqueror
     |         |-konsole-+-bash---su---bash
     |         |         `-bash
     |         `-kwin
     |-kdesktop---kdesktop_lock---xmatrix
     |-kdesud
     |-kdm-+-X
     |     `-kdm---startkde---kwrapper
[...]
```

El parámetro `-p` añade el ID de proceso a un nombre dado. Para que se muestren también las líneas de comandos, utilice el parámetro `-a`:

6.9 Usuarios y acciones `w`

Con el comando `w`, descubra quién ha iniciado sesión en el sistema y qué hace cada usuario. Por ejemplo:

```
tester@linux:~> w
 16:33:03 up  3:33,  2 users,  load average: 0.14, 0.06, 0.02
USER     TTY        LOGIN@   IDLE   JCPU   PCPU WHAT
tester   :0       16:33   ?xdm?   9.42s  0.15s /bin/sh /opt/kde3/bin/startkde
tester   pts/0     15:59    0.00s  0.19s  0.00s w
```

Si usuarios de otros sistemas han iniciado sesión de forma remota, el parámetro `-f` muestra los equipos desde los que han establecido la conexión.

6.10 Utilización de la memoria: `free`

La utilidad `free` examina la utilización de la RAM. Se muestra información detallada acerca de la memoria libre y utilizada (y las áreas de intercambio):

```
ester@linux:~> free
             total       used       free     shared    buffers     cached
Mem:        515584     501704      13880          0      73040     334592
-/+ buffers/cache:      94072     421512
Swap:       658656          0     658656
```

Las opciones `-b`, `-k`, `-m`, `-g` muestran la salida en bytes, KB, MB o GB, respectivamente. El parámetro `-d delay` garantiza que la pantalla se actualiza cada *`delay`* segundos. Por ejemplo, `free -d 1.5` produce una actualización cada 1,5 segundos.

6.11 Buffer de anillo del núcleo: `dmesg`

El núcleo de Linux mantiene ciertos mensajes en un buffer de anillo. Para ver estos mensajes, introduzca el comando `dmesg`:

```
$ dmesg
[...]
end_request: I/O error, dev fd0, sector 0
subfs: unsuccessful attempt to mount media (256)
e100: eth0: e100_watchdog: link up, 100Mbps, half-duplex
```

```
NET: Registered protocol family 17
IA-32 Microcode Update Driver: v1.14 <tigran@veritas.com>
microcode: CPU0 updated from revision 0xe to 0x2e, date = 08112004
IA-32 Microcode Update Driver v1.14 unregistered
bootsplash: status on console 0 changed to on
NET: Registered protocol family 10
Disabled Privacy Extensions on device c0326ea0(lo)
IPv6 over IPv4 tunneling driver
powernow: This module only works with AMD K7 CPUs
bootsplash: status on console 0 changed to on
```

Los eventos más antiguos se registran en los archivos `/var/log/messages` y `/var/log/warn`.

6.12 Sistemas de archivos y su utilización: `mount`, `df` y `du`

El comando `mount` muestra qué sistema de archivos (dispositivo y tipo) se monta en qué punto de montaje:

```
tester@linux:~> mount
/dev/hda3 on / type reiserfs (rw,acl,user_xattr)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
udev on /dev type tmpfs (rw)
devpts on /dev/pts type devpts (rw,mode=0620,gid=5)
/dev/hda1 on /boot type ext2 (rw,acl,user_xattr)
/dev/hda4 on /local type reiserfs (rw,acl,user_xattr)
/dev/fd0 on /media/floppy type subfs
(rw,nosuid,nodev,noatime,fs=floppyfss,procuid)
```

Obtenga información acerca de la utilización total de los sistemas de archivos con el comando `df`. El parámetro `-h` (o `--human-readable`) transforma la salida en un formato legible para los usuarios habituales.

```
tester@linux:~> df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/hda3              11G  3.2G  6.9G  32% /
udev                  252M  104K  252M   1% /dev
/dev/hda1              16M  6.6M  7.8M  46% /boot
/dev/hda4              27G   34M   27G   1% /local
```

Muestre el tamaño total de todos los archivos de un directorio dado y sus subdirectorios con el comando `du`. El parámetro `-s` elimina la salida de información detallada. `-h` transforma de nuevo los datos en un formato legible para usuarios no expertos:

```
tester@linux:~> du -sh /local
1.7M    /local
```

6.13 Sistema de archivos /proc

El sistema de archivos `/proc` es un pseudosistema de archivos en el que el núcleo reserva información importante en forma de archivos virtuales. Por ejemplo, muestre el tipo de CPU con este comando:

```
ester@linux:~> cat /proc/cpuinfo
processor       : 0
vendor_id       : AuthenticAMD
cpu family      : 6
model           : 8
model name      : AMD Athlon(tm) XP 2400+
stepping        : 1
cpu MHz         : 2009.343
cache size      : 256 KB
fdiv_bug        : no
[...]
```

La asignación y el uso de interrupciones se pueden consultar con el siguiente comando:

```
tester@linux:~> cat /proc/interrupts
           CPU0
  0:    3577519          XT-PIC  timer
  1:        130          XT-PIC  i8042
  2:          0          XT-PIC  cascade
  5:     564535          XT-PIC  Intel 82801DB-ICH4
  7:          1          XT-PIC  parport0
  8:          2          XT-PIC  rtc
  9:          1          XT-PIC  acpi, uhci_hcd:usb1, ehci_hcd:usb4
 10:          0          XT-PIC  uhci_hcd:usb3
 11:      71772          XT-PIC  uhci_hcd:usb2, eth0
 12:     101150          XT-PIC  i8042
 14:      33146          XT-PIC  ide0
 15:     149202          XT-PIC  ide1
NMI:          0
LOC:          0
ERR:          0
MIS:          0
```

Algunos de los archivos importantes y su contenido son:

`/proc/devices`
: dispositivos disponibles

`/proc/modules`
: módulos del núcleo cargados

`/proc/cmdline`
: línea de comandos del núcleo

`/proc/meminfo`
: información detallada acerca de la utilización de la memoria

`/proc/config.gz`
: archivo de configuración comprimido `gzip` del núcleo que se ejecuta actualmente

Encontrará más información en el archivo de texto `/usr/src/linux/Documentation/filesystems/proc.txt`. La información acerca de los procesos que se ejecutan actualmente se puede encontrar en los directorios `/proc/`*`NNN`*, donde *`NNN`* es el PID (ID del proceso) del proceso relevante. Todos los procesos pueden encontrar sus propias características en `/proc/self/`:

```
tester@linux:~> ls -l /proc/self
lrwxrwxrwx 1 root root 64 2006-01-09 13:03 /proc/self -> 5356
tester@linux:~> ls -l /proc/self/
total 0
dr-xr-xr-x 2 tester users 0 2006-01-09 17:04 attr
-r-------- 1 tester users 0 2006-01-09 17:04 auxv
-r--r--r-- 1 tester users 0 2006-01-09 17:04 cmdline
lrwxrwxrwx 1 tester users 0 2006-01-09 17:04 cwd -> /home/tester
-r-------- 1 tester users 0 2006-01-09 17:04 environ
lrwxrwxrwx 1 tester users 0 2006-01-09 17:04 exe -> /bin/ls
dr-x------ 2 tester users 0 2006-01-09 17:04 fd
-rw-r--r-- 1 tester users 0 2006-01-09 17:04 loginuid
-r--r--r-- 1 tester users 0 2006-01-09 17:04 maps
-rw------- 1 tester users 0 2006-01-09 17:04 mem
-r--r--r-- 1 tester users 0 2006-01-09 17:04 mounts
-rw-r--r-- 1 tester users 0 2006-01-09 17:04 oom_adj
-r--r--r-- 1 tester users 0 2006-01-09 17:04 oom_score
lrwxrwxrwx 1 tester users 0 2006-01-09 17:04 root -> /
-rw------- 1 tester users 0 2006-01-09 17:04 seccomp
-r--r--r-- 1 tester users 0 2006-01-09 17:04 smaps
-r--r--r-- 1 tester users 0 2006-01-09 17:04 stat
-r--r--r-- 1 tester users 0 2006-01-09 17:04 statm
-r--r--r-- 1 tester users 0 2006-01-09 17:04 status
dr-xr-xr-x 3 tester users 0 2006-01-09 17:04 task
-r--r--r-- 1 tester users 0 2006-01-09 17:04 wchan
```

La asignación de direcciones de ejecutables y de bibliotecas se encuentra en el archivo `maps`:

```
tester@linux:~> cat /proc/self/maps
08048000-0804c000 r-xp 00000000 03:03 17753      /bin/cat
0804c000-0804d000 rw-p 00004000 03:03 17753      /bin/cat
0804d000-0806e000 rw-p 0804d000 00:00 0          [heap]
b7d27000-b7d5a000 r--p 00000000 03:03 11867      \
 /usr/lib/locale/en_GB.utf8/LC_CTYPE
b7d5a000-b7e32000 r--p 00000000 03:03 11868      \
 /usr/lib/locale/en_GB.utf8/LC_COLLATE
b7e32000-b7e33000 rw-p b7e32000 00:00 0
b7e33000-b7f45000 r-xp 00000000 03:03 8837       /lib/libc-2.3.6.so
b7f45000-b7f46000 r--p 00112000 03:03 8837       /lib/libc-2.3.6.so
b7f46000-b7f48000 rw-p 00113000 03:03 8837       /lib/libc-2.3.6.so
b7f48000-b7f4c000 rw-p b7f48000 00:00 0
b7f52000-b7f53000 r--p 00000000 03:03 11842      \
 /usr/lib/locale/en_GB.utf8/LC_NUMERIC
[...]
b7f5b000-b7f61000 r--s 00000000 03:03 9109       \
 /usr/lib/gconv/gconv-modules.cache
b7f61000-b7f62000 r--p 00000000 03:03 9720       \
 /usr/lib/locale/en_GB.utf8/LC_IDENTIFICATION
b7f62000-b7f76000 r-xp 00000000 03:03 8828       /lib/ld-2.3.6.so
b7f76000-b7f78000 rw-p 00013000 03:03 8828       /lib/ld-2.3.6.so
bfd61000-bfd76000 rw-p bfd61000 00:00 0          [stack]
ffffe000-fffff000 ---p 00000000 00:00 0          [vdso]
```

6.13.1 procinfo

El comando `procinfo` resume información importante del sistema de archivos `/proc`:

```
tester@linux:~> procinfo
Linux 2.6.15-rc5-git3-2-default (geeko@buildhost) (gcc 4.1.0 20051129) #1 Wed
 Dec 14 13:10:38 UTC 2005 1CPU [linux.suse.de]

Memory:      Total        Used        Free      Shared     Buffers
Mem:        515584      509472        6112           0       73024
Swap:       658656           0      658656

Bootup: Mon Jan  9 12:59:08 2006    Load average: 0.10 0.04 0.05 1/86 5406

user  :       00:02:070,98   0,8%  page in :     442638  disk 1:    20125r
 13476w
nice  :       00:02:200,91   0,9%  page out:     134950
system:       0:00:42.93   0.3%  page act:      70577
IOwait:       0:01:25.40   0.6%  page dea:      11696
hw irq:       0:00:08.94   0.1%  page flt:    1423622
sw irq:       00:00:010,29   0.0%  swap in :          0
idle  :       04:06:300,54  97,3%  swap out:          0
uptime:       4:13:20.72         context :    3813145

irq  0:   3799268 timer                 irq 8:         2 rtc
```

```
irq 1:       130 i8042 irq  9:         1 acpi, uhci_hcd:usb1,
irq  2:         0 cascade [4]          irq 10:         0 uhci_hcd:usb3
irq  3:         8                      irq 11:     75905 uhci_hcd:usb2, eth0

irq  4:         8                      irq 12:    101150 i8042
irq  5:    564535 Intel 82801DB-ICH4   irq 14:     33733 ide0
irq  6:         9                      irq 15:    157045 ide1
irq  7:         1 parport0 [3]
```

Para ver toda la información, utilice el parámetro `-a`. El parámetro `-nN` actualiza la información cada *N* segundos. En este caso, cierre el programa pulsando Q.

Por defecto, se muestran los valores acumulativos. El parámetro `-d` produce los valores diferenciales. `procinfo -dn5` muestra los valores que han cambiado en los últimos cinco segundos:

6.14 Recursos PCI: `lspci`

El comando `lspci` enumera los recursos PCI:

```
linux:~ # lspci
00:00.0 Host bridge: Intel Corporation 82845G/GL[Brookdale-G]/GE/PE \
 DRAM Controller/Host-Hub Interface (rev 01)
00:01.0 PCI bridge: Intel Corporation 82845G/GL[Brookdale-G]/GE/PE \
 Host-to-AGP Bridge (rev 01)
00:1d.0 USB Controller: Intel Corporation 82801DB/DBL/DBM \
 (ICH4/ICH4-L/ICH4-M) USB UHCI Controller #1 (rev 01)
00:1d.1 USB Controller: Intel Corporation 82801DB/DBL/DBM \
 (ICH4/ICH4-L/ICH4-M) USB UHCI Controller #2 (rev 01)
00:1d.2 USB Controller: Intel Corporation 82801DB/DBL/DBM \
 (ICH4/ICH4-L/ICH4-M) USB UHCI Controller #3 (rev 01)
00:1d.7 USB Controller: Intel Corporation 82801DB/DBM \
 (ICH4/ICH4-M) USB2 EHCI Controller (rev 01)
00:1e.0 PCI bridge: Intel Corporation 82801 PCI Bridge (rev 81)
00:1f.0 ISA bridge: Intel Corporation 82801DB/DBL (ICH4/ICH4-L) \
 LPC Interface Bridge (rev 01)
00:1f.1 IDE interface: Intel Corporation 82801DB (ICH4) IDE \
 Controller (rev 01)
00:1f.3 SMBus: Intel Corporation 82801DB/DBL/DBM (ICH4/ICH4-L/ICH4-M) \
 SMBus Controller (rev 01)
00:1f.5 Multimedia audio controller: Intel Corporation 82801DB/DBL/DBM \
 (ICH4/ICH4-L/ICH4-M) AC'97 Audio Controller (rev 01)
01:00.0 VGA compatible controller: Matrox Graphics, Inc. G400/G450 (rev 85)
02:08.0 Ethernet controller: Intel Corporation 82801DB PRO/100 VE (LOM) \
 Ethernet Controller (rev 81)
```

La utilización de `-v` da como resultado una lista más detallada:

```
linux:~ # lspci
[...]
02:08.0 Ethernet controller: Intel Corporation 82801DB PRO/100 VE (LOM)\
 Ethernet Controller (rev 81)
        Subsystem: Fujitsu Siemens Computer GmbH: Unknown device 1001
        Flags: bus master, medium devsel, latency 66, IRQ 11
        Memory at d1000000 (32-bit, non-prefetchable) [size=4K]
        I/O ports at 3000 [size=64]
        Capabilities: [dc] Power Management version 2
```

La información relativa a la resolución del nombre de dispositivo se obtiene del archivo `/usr/share/pci.ids`. Los IDs de PCI que no aparecen en este archivo están marcados como "Unknown device" (Dispositivo desconocido).

El parámetro `-vv` produce toda la información que el programa podría solicitar. Para ver los valores numéricos puros, debería utilizar el parámetro `-n`.

6.15 Llamadas del sistema para ejecutar un programa: `strace`

La utilidad `strace` le permite efectuar un seguimiento de todas las llamadas del sistema a un proceso que se ejecuta actualmente. Introduzca el comando del modo habitual, añadiendo `strace` al principio de la línea:

```
tester@linux:~> strace ls
execve("/bin/ls", ["ls"], [/* 61 vars */]) = 0
uname({sys="Linux", node="linux", ...}) = 0
brk(0)                                  = 0x805c000
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=89696, ...}) = 0
mmap2(NULL, 89696, PROT_READ, MAP_PRIVATE, 3, 0) = 0xb7ef2000
close(3)                                = 0
open("/lib/librt.so.1", O_RDONLY)       = 3
read(3, "\177ELF\1\1\1\0\0\0\0\0\0\0\0\0\3\0\3\0\1\0\0\0000\36\0"..., 512) \
 = 512
fstat64(3, {st_mode=S_IFREG|0755, st_size=36659, ...}) = 0
[...]
stat64(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 0), ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
 = 0xb7ca7000
write(1, "bin  Desktop  Documents  music\tM"..., 55bin  Desktop  Documents \
 \  music       Music  public_html  tmp
) = 55
close(1)                                = 0
```

```
munmap(0xb7ca7000, 4096)                = 0
exit_group(0)                           = ?
```

Por ejemplo, para saber cuántas veces se ha intentado abrir un archivo en concreto, utilice lo siguiente:

```
tester@linux:~> strace -e open ls .bashrc
open("/etc/ld.so.cache", O_RDONLY)      = 3
open("/lib/librt.so.1", O_RDONLY)       = 3
open("/lib/libacl.so.1", O_RDONLY)      = 3
open("/lib/libc.so.6", O_RDONLY)        = 3
open("/lib/libpthread.so.0", O_RDONLY)  = 3
open("/lib/libattr.so.1", O_RDONLY)     = 3
[...]
```

Para efectuar un seguimiento de todos los procesos secundarios, utilice el parámetro `-f`. El comportamiento y el formato de salida de strace se pueden controlar exhaustivamente. Para obtener información, consulte `man strace`.

6.16 Llamadas de la biblioteca para ejecutar un programa: `ltrace`

El comando `ltrace` le permite efectuar un seguimiento de las llamadas de la biblioteca a un proceso. Este comando se utiliza de un modo similar a `strace`. El parámetro `-c` genera el número y la duración de las llamadas de biblioteca que se han producido:

```
tester@linux:~> ltrace -c find ~
% time     seconds  usecs/call     calls      function
------ ----------- ----------- --------- --------------------
 34.37    6.758937         245     27554 __errno_location
 33.53    6.593562         788      8358 __fprintf_chk
 12.67    2.490392         144     17212 strlen
 11.97    2.353302         239      9845 readdir64
  2.37    0.466754          27     16716 __ctype_get_mb_cur_max
  1.18    0.231189          27      8531 strcpy
  1.17    0.230765          27      8358 memcpy
[...]
  0.00    0.000036          36         1 textdomain
------ ----------- ----------- --------- --------------------
100.00   19.662715                105717 total
```

6.17 Especificación de la biblioteca necesaria: ldd

El comando `ldd` se puede utilizar para buscar qué bibliotecas cargarían el ejecutable dinámico especificado como argumento:

```
tester@linux:~> ldd /bin/ls
        linux-gate.so.1 =>  (0xffffe000)
        librt.so.1 => /lib/librt.so.1 (0xb7f97000)
        libacl.so.1 => /lib/libacl.so.1 (0xb7f91000)
        libc.so.6 => /lib/libc.so.6 (0xb7e79000)
        libpthread.so.0 => /lib/libpthread.so.0 (0xb7e67000)
        /lib/ld-linux.so.2 (0xb7fb6000)
        libattr.so.1 => /lib/libattr.so.1 (0xb7e63000)
```

Los binarios estáticos no requieren bibliotecas dinámicas:

```
tester@linux:~> ldd /bin/sash
        not a dynamic executable
tester@linux:~> file /bin/sash
/bin/sash: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), for
GNU/Linux 2.6.4, statically linked, for GNU/Linux 2.6.4, stripped
```

6.18 Información adicional acerca de los binarios ELF

El contenido de los binarios se puede leer con la utilidad `readelf`. Esto funciona incluso con los archivos ELF creados para otras arquitecturas de hardware:

```
tester@linux:~> readelf --file-header /bin/ls
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF32
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Intel 80386
  Version:                           0x1
  Entry point address:               0x8049b60
  Start of program headers:          52 (bytes into file)
  Start of section headers:          81112 (bytes into file)
  Flags:                             0x0
```

```
  Size of this header:               52 (bytes)
  Size of program headers:           32 (bytes)
  Number of program headers:         9
  Size of section headers:           40 (bytes)
  Number of section headers:         30
  Section header string table index: 29
```

6.19 Comunicación entre procesos: `ipcs`

El comando `ipcs` produce una lista de los recursos IPC que se encuentran actualmente en uso:

```
------ Shared Memory Segments --------
key        shmid      owner      perms      bytes      nattch     status
0x00000000 58261504   tester    600        393216     2          dest
0x00000000 58294273   tester    600        196608     2          dest
0x00000000 83886083   tester    666        43264      2
0x00000000 83951622   tester    666        192000     2
0x00000000 83984391   tester    666        282464     2
0x00000000 84738056   root      644        151552     2          dest

------ Semaphore Arrays --------
key        semid      owner      perms      nsems
0x4d038abf 0          tester    600        8

------ Message Queues --------
key        msqid      owner      perms      used-bytes   messages
```

6.20 Medición del tiempo con `time`

El tiempo que los comandos tardan se puede determinar con la utilidad `time`. Esta utilidad está disponible en dos versiones: como complemento de la shell y como programa (`/usr/bin/time`).

```
tester@linux:~> time find . > /dev/null

real    0m4.051s
user    0m0.042s
sys     0m0.205s
```

Parte 3. Sistema

Aplicaciones de 32 bits y de 64 bits en un entorno de sistema de 64 bits

7

SUSE Linux es compatible con varias plataformas de 64 bits. Esto no significa necesariamente que todas las aplicaciones incluidas se hayan trasladado a plataformas de 64 bits. SUSE Linux admite aplicaciones de 32 bits en entornos de sistema de 64 bits. Este capítulo ofrece una breve descripción general acerca de cómo se implementa esta compatibilidad en las plataformas SUSE Linux de 64 bits y explica cómo ejecutar las aplicaciones de 32 bits (compatibilidad en tiempo de ejecución) y cómo se deben compilar las aplicaciones de 32 bits para que puedan ejecutarse tanto en entornos de sistema de 32 bits como de 64 bits. Además, encontrará información acerca de la API de núcleo y de cómo pueden ejecutarse aplicaciones de 32 bits en un núcleo de 64 bits.

SUSE Linux para plataformas de 64 bits AMD64 y EM64T ha sido diseñado para poder ejecutar las aplicaciones de 32 bits existentes en los entornos de 64 bits "tal cual". Esta compatibilidad hace posible que pueda seguir utilizando sus aplicaciones de 32 bits preferidas sin tener que esperar a que aparezca en el mercado el puerto de 64 bits correspondiente.

7.1 Asistencia sobre tiempo de ejecución

IMPORTANTE: Conflictos entre diferentes versiones de aplicaciones

Si hay una aplicación disponible tanto para entornos de 32 bits como de 64 y se instalan las dos versiones paralelamente, es inevitable que se produzcan

problemas. En estos casos, tendrá que optar por instalar y utilizar sólo una de las dos versiones.

Para que las aplicaciones se puedan ejecutar correctamente, es necesario disponer de ciertas bibliotecas. Desafortunadamente, los nombres de las versiones de 32 bits y 64 bits de estas bibliotecas son idénticos. Es necesario distinguirlos de otra forma.

Para mantener la compatibilidad con la versión de 32 bits, las bibliotecas se almacenan en el mismo sitio del sistema que en el entorno de 32 bits. La versión de 32 bits de `libc.so.6` se encuentra en `/lib/libc.so.6` tanto en el entorno de 32 bits como en el de 64.

Todas las bibliotecas de 64 bits y los archivos de objeto se ubican en directorios llamados `lib64`. Los archivos de objeto de 64 bits que normalmente se suelen encontrar en `/lib`, `/usr/lib` y `/usr/X11R6/lib`, están ahora en `/lib64`, `/usr/lib64` y `/usr/X11R6/lib64`. Esto significa que habrá un lugar reservado para las bibliotecas de 32 bits en `/lib`, `/usr/lib` y `/usr/X11R6/lib` para que no sea necesario cambiar el nombre de archivo para las dos versiones.

Los subdirectorios de los directorios de objeto cuyos datos no dependen del tamaño de palabra no se han cambiado de sitio. Por ejemplo, las fuentes X11 siguen estando en su ubicación habitual, `/usr/X11R6/lib/X11/fonts`. Este esquema sigue las directrices de los estándares LSB (base de estándares de Linux, del inglés Linux Standards Base) y FHS (estándar jerárquico del sistema de archivos, del inglés File System Hierarchy Standard).

7.2 Desarrollo de software

Existe una cadena de herramientas de desarrollo de doble arquitectura que permite generar objetos de 32 bits y de 64 bits. La opción por defecto es compilar objetos de 64 bits, aunque es posible generar objetos de 32 bits mediante indicadores especiales. En GCC, este indicador especial es `-m32`.

Todos los archivos de encabezado deben escribirse de forma independiente de la arquitectura. Las bibliotecas de 32 y 64 bits instaladas deben tener una API (interfaz de programación de aplicaciones) que coincida con los archivos de encabezado instalados. El entorno SUSE normal se ha diseñado siguiendo este principio. En las bibliotecas que haya actualizado manualmente tendrá que resolver estos problemas usted mismo.

7.3 Compilación de software en plataformas de doble arquitectura

En una doble arquitectura, para poder desarrollar binarios para la otra arquitectura es necesario instalar adicionalmente las respectivas bibliotecas para la segunda arquitectura. Estos paquetes se denominan `rpmname-32bit`. También es necesario disponer de los respectivos encabezados y bibliotecas procedentes de los paquetes `rpmname-devel` y de las bibliotecas de desarrollo para la segunda arquitectura procedentes de `rpmname-devel-32bit`.

La mayoría de los programas de código abierto utilizan una configuración basada en el comando `autoconf`. Para utilizar `autoconf` para configurar un programa para la segunda arquitectura, sobrescriba el compilador normal y los ajustes de enlazador de `autoconf` ejecutando el guión `configure` con variables de entorno adicionales.

El ejemplo que sigue hace referencia a un sistema AMD64 o EM64T con x86 como segunda arquitectura:

1. Defina `autoconf` para utilizar el compilador de 32 bits:

   ```
   CC="gcc -m32"
   ```

2. Ordene al enlazador que procese objetos de 32 bits:

   ```
   LD="ld -m elf64_i386"
   ```

3. Defina el ensamblador para que genere objetos de 32 bits:

   ```
   AS="gcc -c -m32"
   ```

4. Indique que las bibliotecas para `libtool` etc. provienen de `/usr/lib`:

   ```
   LDFLAGS="-L/usr/lib"
   ```

5. Indique que las bibliotecas se almacenen en el directorio `lib`:

   ```
   --libdir=/usr/lib
   ```

6. Indique que se utilicen las bibliotecas X de 32 bits:

   ```
   --x-libraries=/usr/X11R6/lib/
   ```

No todos los programas necesitan todas estas variables. Adáptelas al programa en cuestión.

```
CC="gcc -m64"            \
LDFLAGS="-L/usr/lib64;"  \
        .configure       \
          --prefix=/usr  \
          --libdir=/usr/lib64
make
make install
```

7.4 Especificaciones de núcleo

Los núcleos de 64 bits para AMD64 y EM64T ofrecen una interfaz ABI (interfaz binaria de aplicaciones) de núcleo tanto de 64 bits como de 32 bits. Esta última es idéntica a la ABI para el núcleo de 32 bits correspondiente. Esto significa que la aplicación de 32 bits se puede comunicar con el núcleo de 64 bits de la misma forma que con el núcleo de 32 bits.

La emulación de 32 bits de las llamadas del sistema de un núcleo de 64 bits no es compatible con algunas interfaces API que emplean los programas de sistema. Esto dependerá de la plataforma. Por este motivo, un pequeño número de aplicaciones, como `lspci` o los programas de administración LVM, deben compilarse como programas de 64 bits para poder funcionar correctamente.

Los núcleos de 64 bits sólo pueden cargar módulos de núcleos de 64 bits especialmente compilados para este núcleo. No es posible utilizar módulos de núcleos de 32 bits.

SUGERENCIA

Algunas aplicaciones exigen módulos de carga de núcleos independientes. Si tiene intención de utilizar una aplicación de 32 bits en un entorno de sistema de 64 bits, póngase en contacto con el proveedor de esta aplicación y de SUSE para asegurarse de que puede adquirir para este módulo la versión de 64 bits del módulo de carga de núcleos y la versión compilada de 32 bits de la API de núcleo.

Arranque y configuración de un sistema Linux

8

El arranque de un sistema Linux incluye diferentes componentes. Este capítulo describe los principios subyacentes y destaca los componentes incluidos. En este capítulo también se describen el concepto de niveles de ejecución y la configuración del sistema SUSE mediante `sysconfig`.

8.1 Proceso de arranque de Linux

El proceso de arranque de Linux consta de varios pasos cada uno de ellos representado por otro componente. La siguiente lista resume el proceso de arranque y las funciones de los principales componentes relacionados.

1. **BIOS** Después de haber encendido el equipo, la BIOS inicializa la pantalla y el teclado y comprueba la memoria principal. Hasta aquí, la máquina no tiene acceso a ningún medio de almacenamiento masivo. A continuación, la información de la fecha y hora actuales y de los principales periféricos se carga a partir de los valores CMOS. Una vez reconocido el disco duro principal y su geometría, el control de sistema pasa de la BIOS al cargador de arranque.

2. **Cargador de arranque** El primer sector de datos de 512 bytes físicos se carga en la memoria principal y el *cargador de arranque* ubicado al inicio de este sector prevalece. Los comandos ejecutados por el cargador de arranque determinan la parte restante del proceso de arranque. Por lo tanto, los primeros 512 bytes del primer disco duro se consideran como *Registro de inicio principal* (MBR). A continuación, el cargador de arranque traslada el control al sistema operativo en sí, en este caso, el núcleo Linux. Puede encontrar más información

acerca de GRUB, el cargador de arranque de Linux, en el Capítulo 9, *Cargador de arranque* (p. 211).

3. **Núcleo y initramfs** Para pasar el control de sistema, el cargador de arranque carga en la memoria el núcleo y un sistema inicial de archivos basado en RAM (initramfs). El núcleo puede utilizar directamente el contenido del ramfs inicial. El ramfs inicial contiene un pequeño ejecutable denominado init que gestiona el montaje del sistema real de archivos raíz. En las primeras versiones de SUSE Linux, initrd y linuxrc gestionaban respectivamente estas tareas. Para obtener más información acerca de initramfs, consulte la Sección 8.1.1, “initramfs” (p. 194).

4. **init en initramfs** Este programa realiza todas las acciones necesarias para el montaje del sistema de archivos raíz correcto, como proporcionar la función de núcleo para el sistema de archivos necesario y los controladores de dispositivos para los controladores de almacenamiento masivo con udev. Una vez encontrado el sistema de archivos raíz, se comprueban los errores y se realiza el montaje. Si este paso se ha realizado correctamente, initramfs se limpia y el programa init se ejecuta en el sistema de archivos raíz. Para obtener más información acerca de init, consulte la Sección 8.1.2, “init en initramfs” (p. 195). Para obtener más información acerca de udev, consulte el Capítulo 12, *Gestión dinámica de dispositivos de núcleo con udev* (p. 273).

5. **init** init gestiona el arranque actual del sistema mediante diferentes niveles que proporcionan varias funciones. init se describe en la Sección 8.2, “Proceso init” (p. 197).

8.1.1 initramfs

initramfs es un pequeño archivo de reserva de cpio que el núcleo puede cargar en un disco RAM. Proporciona un entorno Linux mínimo que habilita la ejecución de programas antes de que se monte el sistema de archivos raíz. El entorno Linux mínimo se carga en la memoria mediante las rutinas de la BIOS y no necesita requisitos específicos de hardware, únicamente una memoria suficiente. initramfs siempre debe proporcionar un ejecutable denominado init que ejecuta el programa init actual en el sistema de archivos raíz para que se lleve a cabo el proceso de arranque.

Antes de que el actual sistema de archivos raíz se pueda montar y de que el actual sistema operativo se pueda iniciar, el núcleo necesita los controladores correspondientes

para acceder al dispositivo en el que se ubica el sistema de archivos raíz. Estos controladores pueden incluir controladores especiales para algunos tipos de unidades de disco duro o controladores de red para acceder al sistema de archivos en red. Los módulos necesarios para el sistema de archivos raíz se pueden cargar con init o initramfs. Una vez que se cargan los módulos, udev proporciona a initramfs los dispositivos necesarios. initramfs está disponible durante todo el proceso de arranque, lo que hace posible la gestión de todos los eventos de dispositivo generados durante el arranque.

Si necesita cambiar el hardware (discos duros) en un sistema instalado y este hardware requiere controladores diferentes en el núcleo durante el arranque, deberá actualizar initramfs. Esto se realiza de la misma manera que con el predecesor de initramfs, initrd, es decir, llamando a `mkinitrd`. Al llamar a `mkinitrd` sin ningún argumento se crea un initramfs. Al llamar `mkinitrd -R` se crea un initrd. En SUSE Linux, los módulos para cargar se especifican mediante la variable `INITRD_MODULES` en `/etc/sysconfig/kernel`. Después de la instalación, esta variable se establece en su valor correcto. Los módulos se cargan exactamente en el mismo orden en el que aparecen en `INITRD_MODULES`. Esto es especialmente importante si se utilizan varios controladores SCSI, porque, si no, los nombres de los discos duros cambiarían. Estrictamente hablando, sería suficiente cargar sólo los controladores necesarios para acceder al sistema de archivos raíz. Sin embargo, todos los controladores SCSI necesarios para la instalación se cargan mediante initramfs o initrd porque si no, después, la carga podría generar problemas.

IMPORTANTE: Actualización de initramfs o initrd

El cargador de arranque carga initramfs o initrd de la misma manera que el núcleo. No es necesario volver a instalar GRUB después de actualizar initramfs o initrd, puesto que, al arrancar, GRUB busca en el directorio el archivo correcto.

8.1.2 init en initramfs

El propósito principal de init en initramfs es preparar el montaje y el acceso al sistema de archivos raíz real. En función de la configuración del sistema actual, init es responsable de las tareas siguientes.

Carga de módulos de núcleo
: En función de la configuración de hardware, se necesitarán controladores especiales para acceder a los componentes de hardware de su equipo (el componente más

importante es la unidad de disco duro). Para acceder al sistema de archivos raíz final, el núcleo necesita cargar los controladores del sistema de archivos correctos.

Provisión de archivos de bloque especiales
: Para cada módulo cargado, el núcleo genera eventos de dispositivo. udev gestiona estos eventos y genera los archivos especiales de dispositivo en un sistema de archivos RAM en `/dev`. Sin esos archivos especiales, no se podría acceder al sistema de archivos.

Gestión de las configuraciones RAID y LVM
: Si configura el sistema para almacenar el sistema de archivos raíz en RAID o LVM, init configura LVM o RAID para habilitar el posterior acceso al sistema de archivos raíz. Se puede encontrar información acerca de RAID en la Sección 2.2, “Configuración de RAID de software” (p. 64). Se puede encontrar información acerca de LVM en la Sección 2.1, “Configuración de LVM” (p. 57).

Gestión de la configuración de red
: Si ha configurado el sistema para utilizar un sistema de archivos raíz montado en red (montado mediante NFS), init debe comprobar que los controladores de red adecuados estén cargados y configurados para permitir el acceso al sistema de archivos raíz.

Cuando se llama a init durante el arranque inicial como parte del proceso de instalación, sus tareas son diferentes de las mencionadas anteriormente:

Búsqueda del medio de instalación
: Al iniciar el proceso de instalación, la máquina carga un núcleo de instalación y un initrd especial mediante el instalador YaST y a partir del medio de instalación. El instalador YaST, que se ejecuta en un sistema de archivos RAM, necesita información acerca de la ubicación actual del medio de instalación para acceder a él e instalar el sistema operativo.

Inicio del reconocimiento de hardware y carga de los módulos de núcleo adecuados
: Tal y como se ha mencionado en la Sección 8.1.1, “initramfs” (p. 194), el proceso de arranque se inicia con un conjunto mínimo de controladores que se pueden utilizar con casi todas las configuraciones de hardware. init inicia un proceso de escaneo de hardware inicial que determina el conjunto de controladores adecuado para la configuración del hardware. Estos valores se escriben después en `INITRD_MODULES`, incluido en `/etc/sysconfig/kernel`, con el fin de habilitar cualquier proceso de arranque posterior para que use un initrd persona-

lizado, o en un archivo `/etc/sysconfig/hardware/hwconfig-*` si el dispositivo no es necesario durante el proceso de arranque. Durante el proceso de instalación, init carga este conjunto de módulos.

Carga del sistema de instalación o del sistema de rescate
: En cuanto se haya reconocido correctamente el hardware, se hayan cargado los controladores adecuados y udev haya creado los archivos especiales de dispositivo, init inicia el sistema de instalación, que contiene el instalador YaST en sí, o el sistema de rescate.

Inicio de YaST
: Por último, init inicia YaST, que inicia la instalación del paquete y la configuración del sistema.

8.2 Proceso init

El programa init, cuyo ID de proceso es el 1, es responsable de iniciar el sistema en el modo requerido y desempeña además una función especial. Se inicia directamente mediante el núcleo y resiste la señal 9, que generalmente cierra todos los procesos. Los demás programas se inician directamente mediante init o mediante uno de sus subprocesos.

init se configura en el archivo `/etc/inittab` en el que están definidos los *niveles de ejecución* (consulte la Sección 8.2.1, “Niveles de ejecución” (p. 197)). El archivo también especifica qué servicios y daemons están disponibles para cada uno de los niveles. En función de las entradas en `/etc/inittab`, init ejecutará varios guiones. Por razones de claridad, estos guiones, denominados *init scripts*, están ubicados en el directorio `/etc/init.d` (consulte la Sección 8.2.2, “Guiones init” (p. 200)).

init se encarga de todo el proceso de encendido y apagado del sistema. Desde este punto de vista, el núcleo se puede considerar un proceso en segundo plano cuya tarea es mantener el resto de procesos y ajustar el tiempo de la CPU y el acceso de hardware en función de las peticiones de otros programas.

8.2.1 Niveles de ejecución

En Linux, los *niveles de ejecución* definen cómo se inicia el sistema y qué servicios están disponibles en el sistema en funcionamiento. Después del arranque, el sistema se

inicia tal y como se ha explicado en `/etc/inittab` en la línea `initdefault`. Generalmente, esto es `3` o `5`. Consulte la Tabla 8.1, “Niveles de ejecución disponibles” (p. 198). Como alternativa, el nivel de ejecución se puede especificar durante el arranque (por ejemplo, en el indicador de inicio). Los parámetros que el núcleo no evalúa directamente pasan a init.

Tabla 8.1 *Niveles de ejecución disponibles*

Nivel de ejecución	Descripción
0	Parada del sistema
propiedades	Modo monousuario; en el indicador de inicio, sólo para asignaciones de teclado de EE.UU.
1	Modo monousuario
2	Modo multiusuario local sin red remota (NFS, etc.)
3	Modo multiusuario completo con red
4	No utilizado
5	Modo multiusuario completo con red y gestor de pantalla X (KDM, GDM o XDM)
6	Reinicio del sistema

IMPORTANTE: evite el nivel de ejecución 2 con una partición montada a través de NFS

No se debe utilizar el nivel de ejecución 2 si el sistema monta una partición como `/usr` a través de NFS. El sistema podría comportarse de modo inesperado si faltan archivos de programa o bibliotecas debido a que el servicio NFS no está disponible en el modo de ejecución 2 (modo multiusuario local sin red remota).

Para cambiar los niveles de ejecución mientras el sistema se esté ejecutando, introduzca `telinit` y el número correspondiente como argumento. Únicamente el administrador

del sistema tiene permiso para realizar esta operación. La siguiente lista resume los comandos más importantes del área de niveles de ejecución.

`telinit 1` o `shutdown now`
: El sistema cambia a *modo monousuario*. Este modo se utiliza para las tareas de administración y mantenimiento del sistema.

`telinit 3`
: Todos los programas y servicios fundamentales (incluida la red) se inician y los usuarios normales pueden iniciar sesión y trabajar en el sistema sin necesidad de un entorno gráfico.

`telinit 5`
: Se habilita el entorno gráfico. Normalmente se inicia un gestor de pantalla como XDM, GDM o KDM. Si está habilitado el inicio de sesión automático, se inicia la sesión del usuario local en el gestor de ventanas preseleccionado (GNOME, KDE o cualquier otro gestor de ventanas).

`telinit 0` o `shutdown -h now`
: El sistema se detiene.

`telinit 6` o `shutdown -r now`
: El sistema se detiene y, a continuación, se reinicia.

El nivel de ejecución `5` es el nivel por defecto en todas las instalaciones estándar SUSE Linux. Se solicita a los usuarios que inicien la sesión con una interfaz gráfica o se inicia la sesión del usuario por defecto automáticamente. El nivel de ejecución por defecto es `3`, X Window System debe configurarse correctamente, tal y como se describe en el Capítulo 14, *El sistema X Window* (p. 293), antes de que el nivel de ejecución pase a `5`. A continuación, compruebe si el sistema funciona como se espera introduciendo `telinit 5`. Si todo funciona tal y como se espera, puede utilizar YaST para establecer el nivel de ejecución por defecto en `5`.

Generalmente, ocurren dos cosas al cambiar los niveles de ejecución. En primer lugar, se inician los guiones de detención del nivel de ejecución actual al mismo tiempo que se cierran algunos programas fundamentales para el nivel de ejecución. A continuación, se inician los guiones de inicio del nuevo nivel de ejecución. En este paso y en la mayoría de los casos, se inician algunos programas. Por ejemplo, al cambiar del nivel de ejecución 3 al 5, sucede lo siguiente:

1. El administrador (`root`) solicita a init que cambie a un nivel de ejecución diferente introduciendo `telinit 5`.

2. init consulta su propio archivo de configuración (`/etc/inittab`) y determina si debe iniciar `/etc/init.d/rc` con el nuevo nivel de ejecución como parámetro.

3. Ahora `rc` llama a todos los guiones de detención del nivel de ejecución actual, pero en el nivel de ejecución nuevo, sólo a aquéllos para los que no existe un guión de inicio. En este ejemplo, aparecen todos los guiones ubicados en `/etc/init.d/rc3.d` (el nivel de ejecución antiguo era 3) y que comiencen por la letra `K`. El número que sigue a la letra `K` especifica el orden de inicio, puesto que es necesario tener en cuenta algunas dependencias.

4. Los últimos elementos que se inician son los guiones de inicio del nivel de ejecución nuevo. En este ejemplo, éstos se ubican en `/etc/init.d/rc5.d` y comienzan con `S`. Aquí, también se aplica el mismo procedimiento para el orden en el que se inician.

Al cambiar al mismo nivel de ejecución que el actual, init sólo comprueba si existen cambios en `/etc/inittab` y lleva a cabo los pasos adecuados, por ejemplo, para iniciar un `getty` en otra interfaz. Se puede conseguir la misma funcionalidad con el comando `telinit q`.

8.2.2 Guiones init

Existen dos tipos de guiones en `/etc/init.d`:

Guiones ejecutados directamente por init
: Únicamente durante el proceso de arranque o si el sistema se ha apagado de forma inmediata (debido a un fallo en la alimentación o si el usuario ha pulsado Ctrl + Alt + Del). La ejecución de estos guiones se describe en `/etc/inittab`.

Guiones ejecutados indirectamente por init
: Se ejecutan al cambiar el nivel de ejecución y siempre llaman al guión maestro `/etc/init.d/rc`, que garantiza el orden correcto de los guiones correspondientes.

Todos los guiones se ubican en `/etc/init.d`. Para llamar a los guiones que se ejecutan durante el arranque, se utilizan enlaces simbólicos de `/etc/init.d/boot`

`.d`. Para llamar a los guiones que se encargan de cambiar el nivel de ejecución, se utilizan enlaces simbólicos desde un subdirectorio (de `/etc/init.d/rc0.d` a `/etc/init.d/rc6.d`). Esto se debe a razones de claridad y evita la creación de guiones duplicados al utilizarlos en varios niveles de ejecución. Puesto que cada guión se puede ejecutar como guión de inicio o de detención, estos guiones deben poder admitir los parámetros de `start` y `stop`. Los guiones también admiten las opciones `restart` (reiniciar), `actualizar`, `force-reload` (forzar-actualizar) y `estado`. Estas opciones se explican en la Tabla 8.2, "Posibles opciones del guión init" (p. 201). Los guiones ejecutados directamente mediante init no disponen de estos enlaces. Cuando sea necesario, se ejecutan de forma independiente desde el nivel de ejecución.

Tabla 8.2 *Posibles opciones del guión init*

Opción	Descripción
`start`	Inicia el servicio.
`stop`	Detiene el servicio.
`restart`	Si el servicio está en funcionamiento, lo detiene y, a continuación, lo reinicia. Si no está en funcionamiento, lo inicia.
`actualizar`	Actualiza la configuración sin detener ni reiniciar el servicio.
`force-reload` (`forzar-actualizar`)	Actualiza la configuración si el servicio es compatible con esta función. De lo contrario, realiza lo mismo que si la opción fuese `restart` (reiniciar).
`status`	Muestra el estado actual del servicio.

Los enlaces de cada subdirectorio específico del nivel de ejecución permiten asociar guiones a diferentes niveles de ejecución. Al instalar o desinstalar los paquetes, estos enlaces se agregan y se eliminan mediante el insserv del programa (o utilizando `/usr/lib/lsb/install_initd`, guión que ejecuta este programa). Para obtener más información, consulte la página Man de insserv(8).

A continuación, se ofrece una introducción corta de los guiones de arranque y detención ejecutados en primer o último lugar, así como una explicación del guión de mantenimiento.

`boot`
: Ejecutado al iniciar el sistema directamente mediante init. Es independiente del nivel de ejecución seleccionado y sólo se ejecuta una vez. Aquí, se montan los sistemas de archivos `proc` y `pts` y se activa blogd (daemon de inicio de sesión de arranque). Si se arranca el sistema por primera vez después de una actualización o una instalación, se inicia la configuración del sistema inicial.

  El daemon blogd es un servicio iniciado por boot y rc antes que cualquier otro. Se detiene una vez completadas las acciones originadas por los guiones anteriores (por ejemplo, ejecución de varios guiones). blogd escribe cualquier salida de pantalla en el archivo de registro `/var/log/boot.msg`, pero sólo si `/var` está montado en lectura-escritura. De lo contrario, blogd mantiene en el búfer todos los datos de la pantalla hasta que `/var` esté disponible. Puede obtener más información acerca de blogd en la página Man de blogd(8).

  El guión `boot` también se encarga del inicio de todos los guiones en `/etc/init.d/boot.d` con un nombre que empieza por `S`. Los sistemas de archivos se comprueban y los dispositivos loop se configuran si fuese necesario. También se establece la hora del sistema. Si se produce un error durante la comprobación y la reparación automática del sistema de archivos, el gestor del sistema puede intervenir después de haber introducido la contraseña root. El último guión ejecutado es el `boot.local`.

`boot.local`
: Introduzca aquí los comandos adicionales para ejecutar durante el arranque antes de cambiar a un nivel de ejecución. Se puede comparar a `AUTOEXEC.BAT` en sistemas DOS.

`boot.setup`
: Este guión se ejecuta al cambiar del modo monousuario a cualquier otro nivel de ejecución y es responsable de varios ajustes básicos, como la distribución del teclado y la inicialización de las consolas virtuales.

`halt`
: Este guión sólo se ejecuta durante el cambio al nivel de ejecución 0 o 6. Se ejecuta como `halt` o como `reboot`. El apagado o la reinicialización del sistema dependen de como se ha ejecutado `halt`.

`rc`
: Este guión ejecuta los guiones adecuados del nivel de ejecución actual e inicia los guiones del nuevo nivel de ejecución seleccionado.

Puede crear sus propios guiones e integrarlos fácilmente en el esquema descrito anteriormente. Si desea obtener instrucciones sobre el formato, el nombre y la organización de guiones personalizados, consulte las especificaciones de LSB y las páginas Man de `init`, `init.d` e `insserv`. También puede consultar las páginas Man de `startproc` y `killproc`.

AVISO: Los guiones init incorrectos pueden detener el sistema.

Los guiones init incorrectos pueden bloquear la máquina. Edite esos guiones con cuidado y, si es posible, realice una comprobación exhaustiva en el entorno multiusuario. Puede encontrar información útil acerca de los guiones init en la Sección 8.2.1, “Niveles de ejecución” (p. 197).

Para crear un guión init personalizado para un determinado programa o servicio, utilice como plantilla el archivo `/etc/init.d/skeleton`. Guarde una copia de este archivo con un nombre nuevo y edite el programa y los nombres de archivos, las vías y otros detalles correspondientes si fuese necesario. Puede que necesite mejorar el guión con código propio, por lo que las acciones correctas se originan mediante el procedimiento init.

El bloque `INIT INFO` de la parte superior es un componente necesario del guión y debe editarse. Consulte el Ejemplo 8.1, “Bloque INIT INFO mínimo” (p. 203).

Ejemplo 8.1 *Bloque INIT INFO mínimo*

```
### BEGIN INIT INFO
# Provides:          FOO
# Required-Start:    $syslog $remote_fs
# Required-Stop:     $syslog $remote_fs
# Default-Start:     3 5
# Default-Stop:      0 1 2 6
# Description:       Start FOO to allow XY and provide YZ
### END INIT INFO
```

En la primera línea del bloque `INFO`, después de `Provides:`, especifique el nombre del programa o servicio controlado por el guión init. En las líneas `Required-Start:` y `Required-Stop:`, especifique todos los servicios que deban iniciarse o detenerse antes de que se inicie o se detenga el propio servicio. Esta información se utilizará más adelante para generar la numeración de los nombres de guiones, tal y como aparecen en los directorios del nivel de ejecución. Después de `Default-Start:` y `Default-Stop:`, especifique los niveles de ejecución en los que el servicio debería iniciarse o detenerse automáticamente. Por último, en `Description:`, proporcione una descripción corta del servicio en cuestión.

Para crear los enlaces desde los directorios de nivel de ejecución (`/etc/init.d/rc?.d/`) a los guiones correspondientes en `/etc/init.d/`, introduzca el comando `insserv` *`new-script-name`*. El programa insserv evalúa el encabezado `INIT INFO` para crear los enlaces necesarios para iniciar y detener guiones en los directorios de nivel de ejecución (`/etc/init.d/rc?.d/`). El programa también se encarga del orden de inicio y detención correcto de cada nivel de ejecución al incluir los números necesarios en los nombres de los enlaces. Si prefiere una herramienta gráfica para crear dichos enlaces, utilice el editor de niveles de ejecución proporcionado por YaST, tal y como se describe en la Sección 8.2.3, “Configuración de los servicios de sistema (nivel de ejecución) mediante YaST” (p. 204).

Si un guión que ya aparece en `/etc/init.d/` debe integrarse en el esquema de nivel de ejecución existente, cree los enlaces en los directorios de nivel de ejecución mediante insserv o habilitando el correspondiente servicio en el editor de niveles de ejecución de YaST. Los cambios que haya realizado se aplicarán durante el siguiente arranque; el nuevo servicio se iniciará automáticamente.

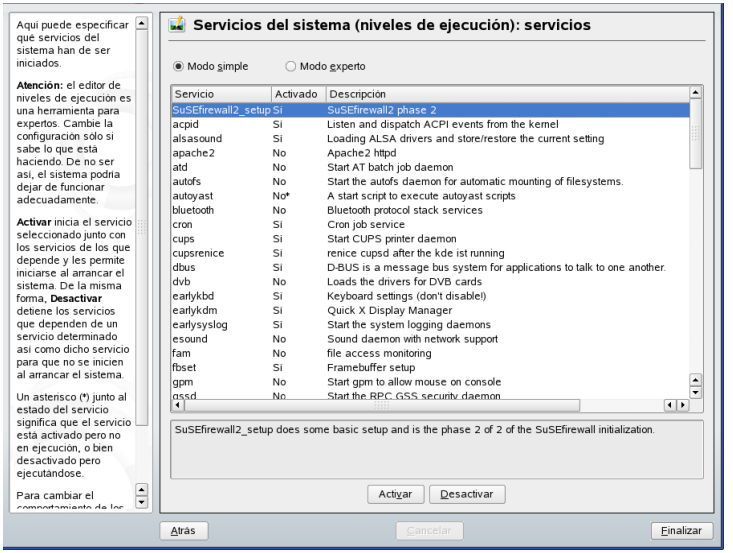
No establezca estos enlaces de forma manual. Si algo no funciona en el bloque `INFO`, surgirán problemas cuando se ejecute `insserv` más adelante para algún otro servicio. El servicio que se añade manualmente se suprimirá cuando se vuelva a ejecutar `insserv`.

8.2.3 Configuración de los servicios de sistema (nivel de ejecución) mediante YaST

Después de iniciar el módulo YaST mediante *YaST → Sistema → Servicios del sistema (niveles de ejecución)*, éste muestra una descripción general que enumera todos los

servicios disponibles y el estado actual de cada servicio (inhabilitado o habilitado). Decida si desea utilizar el módulo en *Modo simple* o en *Modo avanzado*. El *Modo simple* por defecto debe ser suficiente para la mayoría de finalidades. La columna de la izquierda muestra el nombre del servicio, la columna del centro indica su estado actual y la de la derecha proporciona una descripción corta. Para el servicio seleccionado, se proporciona una descripción detallada en la parte inferior de la ventana. Para habilitar un servicio, selecciónelo en la tabla y, a continuación, elija *Habilitar*. Se aplican los mismos pasos para inhabilitar un servicio.

Figura 8.1 *Servicios de sistema (nivel de ejecución)*



Para llevar a cabo un control detallado de los niveles de ejecución en los que se inicia o se detiene el servicio, o para cambiar el nivel de ejecución por defecto, primero seleccione *Modo avanzado*. En la parte superior aparecerá el nivel de ejecución por defecto en curso o “initdefault” (el nivel de ejecución en el que se arranca por defecto el sistema). Generalmente, el nivel de ejecución por defecto de un sistema SUSE Linux es el 5 (modo multiusuario completo con red y X). Otra opción podría ser el nivel de ejecución 3 (modo multiusuario completo con red).

El cuadro de diálogo YaST permite seleccionar uno de los niveles de ejecución (tal y como aparecen en la lista de la Tabla 8.1, “Niveles de ejecución disponibles” (p. 198)) como el nuevo nivel por defecto. Además, utiliza la tabla de esta ventana para habilitar o inhabilitar servicios y daemons individuales. La tabla enumera los servicios y daemons

disponibles, muestra si están actualmente habilitados en el sistema y, si es así, en qué niveles de ejecución. Después de haber seleccionado una de las filas con el ratón, haga clic en las casillas de verificación que representan los niveles de ejecución (*B*, *0*, *1*, *2*, *3*, *5*, *6* y *S*) para definir los niveles en los que el servicio o daemon seleccionado debería ejecutarse. El nivel de ejecución 4 no está inicialmente definido para permitir la creación de un nivel personalizado. A continuación, en la descripción general de la tabla, se proporciona una descripción corta del actual servicio o daemon seleccionado.

Mediante *Start (Iniciar), Detener o Actualizar*, decida si se debe activar un servicio. *Refrescar estado* comprueba el estado actual. *Set or Reset* (Ajustar o Reajustar) le permite seleccionar si desea aplicar los cambios al sistema o restaurar los ajustes existentes antes de iniciar el editor de nivel de ejecución. Al seleccionar *Finalizar* se guardarán los ajustes modificados en el disco.

AVISO: Los ajustes de nivel de ejecución incorrectos pueden dañar el sistema.

Los ajustes de nivel de ejecución incorrectos pueden inhabilitar el sistema. Antes de aplicar los cambios, asegúrese de que conoce las consecuencias.

8.3 Configuración del sistema mediante /etc/sysconfig

La configuración principal de SUSE Linux está controlada mediante los archivos de configuración de `/etc/sysconfig`. Sólo los guiones correspondientes pueden leer los archivos individuales de `/etc/sysconfig`. Esto garantiza que la configuración de la red, por ejemplo, sólo necesite ser analizada por los guiones relacionados a la red. Otros archivos de configuración de sistema se generan en función de la configuración de `/etc/sysconfig`. SuSEconfig lleva a cabo esta tarea. Por ejemplo, si modifica la configuración de red, SuSEconfig también podrá realizar cambios en el archivo `/etc/host.conf`, puesto que es uno de los archivos correspondientes para la configuración de la red. Este concepto le permite realizar cambios básicos en la configuración sin necesidad de reiniciar el sistema.

Existen dos modos de editar la configuración del sistema. Mediante el editor YaST sysconfig o editando los archivos de configuración de forma manual.

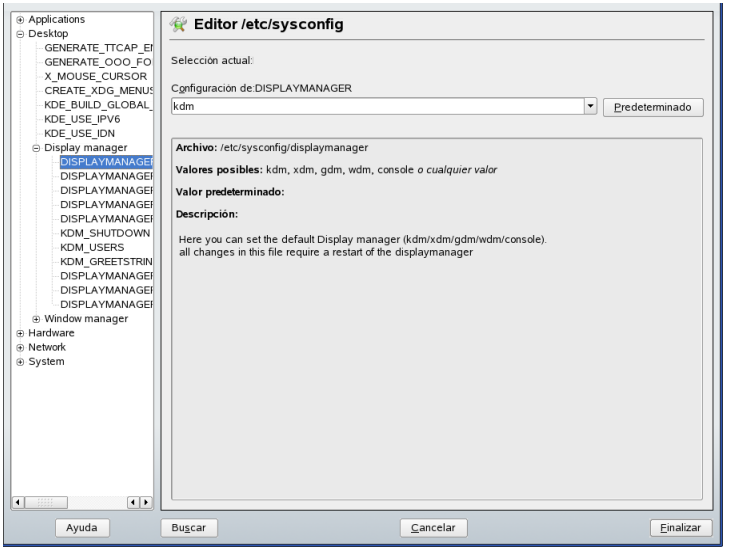
8.3.1 Cambio de la configuración del sistema mediante el editor YaST sysconfig

El editor YaST sysconfig proporciona una interfaz de la configuración del sistema fácil de utilizar. No son necesarios conocimientos previos de la ubicación actual de la variable de configuración que necesite modificar, puede utilizar la función de búsqueda incorporada de este módulo, cambiar el valor de la variable de configuración y dejar que YaST se encargue de aplicar los cambios al actualizar las configuraciones que dependen de los valores establecidos en `sysconfig` y al reinicializar los servicios.

AVISO: La modificación de archivos /etc/sysconfig/* puede dañar la instalación

No modifique los archivos `/etc/sysconfig` si no dispone de la experiencia ni de los conocimientos necesarios. Puede provocar daños considerables en el sistema. Los archivos de `/etc/sysconfig` incluyen un comentario corto para cada variable que explica el efecto que ésta provoca.

Figura 8.2 *Configuración del sistema mediante el editor sysconfig*



El cuadro de diálogo YaST sysconfig está dividido en tres partes. La parte izquierda del cuadro de dialogo muestra una vista de árbol de todas las variables de configuración. Al seleccionar una variable, la parte de la derecha muestra la selección actual y la configuración actual de la variable. Debajo, una tercera ventana muestra una descripción corta del propósito de la variable, de los valores posibles, del valor por defecto y del archivo de configuración actual que origina la variable. El cuadro de diálogo también muestra información acerca de qué guión de configuración se ejecuta después de cambiar la variable y qué nuevo servicio se inicia como resultado del cambio. YaST le solicita que confirme los cambios y le informa de los guiones que se ejecutarán después de salir del cuadro de dialogo al seleccionar *Finalizar*. También selecciona los servicios y guiones que se van a omitir de momento, por lo que se iniciarán más tarde. YaST aplica todos los cambios de forma automática y reinicia cualquier servicio relacionado para que los cambios surtan efecto.

8.3.2 Cambio de la configuración del sistema de forma manual

Para cambiar la configuración del sistema de forma manual, siga estos pasos

1. Convierta el sistema en `root`.

2. Ponga el sistema en modo monousuario (nivel de ejecución 1) mediante `init 1`.

3. Cambie los archivos de configuración como desee mediante un editor de su elección.

   Si no utiliza YaST para cambiar los archivos de configuración en `/etc/sysconfig`, asegúrese de que los valores de variables vacías están representados por comillas (`KEYTABLE=""`) y que los valores con espacios incluidos en estas variables están entre comillas. Los valores que se componen de una sola palabra no necesitan comillas.

4. Ejecute `SuSEconfig` para asegurarse de que se realizan los cambios.

5. Vuelva a pasar el sistema al nivel de ejecución anterior mediante un comando de tipo `init` *`default_runlevel`*. Sustituya *`default_runlevel`* por el nivel de ejecución por defecto del sistema. Seleccione `5` si desea volver al

modo multiusuario completo con red y X o elija `3` si prefiere trabajar en modo multiusuario con red.

Este procedimiento es importante al cambiar la configuración de systemwide, así como la configuración de red. Los pequeños cambios no deberían requerir que se cambie el sistema al modo monousuario, pero puede hacerlo si desea asegurarse de que todos los programas relacionados se reinicien correctamente.

SUGERENCIA: Establecimiento de la configuración automática del sistema

Para inhabilitar la configuración automática del sistema mediante SuSEconfig, establezca la variable `ENABLE_SUSECONFIG` de `/etc/sysconfig/suseconfig` en no. No inhabilite SuSEconfig si desea utilizar el soporte de instalación SUSE. También es posible inhabilitar la configuración automática de forma parcial.

9 Cargador de arranque

Este capítulo describe cómo configurar GRUB (Gran gestor de arranque unificado), el cargador de arranque utilizado en SUSE Linux. Hay un módulo YaST especial disponible para llevar a cabo toda la configuración. Si no está familiarizado con el arranque en Linux, lea las siguientes secciones para adquirir información general. Este capítulo también describe algunos de los problemas que se encuentran frecuentemente al arrancar con GRUB y sus soluciones.

Este capítulo se centra en la gestión del arranque y en la configuración del cargador de arranque GRUB. El procedimiento de arranque en su totalidad se explica en el Capítulo 8, *Arranque y configuración de un sistema Linux* (p. 193). Un cargador de arranque representa la interfaz entre la máquina (BIOS) y el sistema operativo (SUSE Linux). La configuración del cargador de arranque tiene un impacto directo en el inicio del sistema operativo.

Los siguientes términos aparecen con frecuencia en este capítulo y pueden necesitar alguna explicación:

Registro de arranque principal (MBR)
: La estructura del MBR está definida por una convención independiente del sistema operativo. Los primeros 446 bytes se reservan para el código del programa. Por lo general almacenan el programa del cargador de arranque, en este caso, GRUB stage 1. Los 64 bytes siguientes proporcionan espacio para una tabla de partición con hasta cuatro entradas (consulte “Tipos de partición” (Capítulo 1, *Instalación mediante YaST*, ↑Inicio)). La tabla de partición contiene información acerca del particionamiento del disco duro y del tipo de sistema de archivos. El sistema operativo necesita esta tabla para gestionar el disco duro. Con GRUB stage 1 en el MBR, una partición exacta se debe marcar como *activa.* Los dos últimos bytes del

MBR deben contener un “número mágico” estático (AA55). El BIOS no considera válidos los MBR que tengan un valor distinto.

Sectores de arranque
: Los sectores de arranque son los primeros sectores de las particiones del disco duro, con la excepción de la partición extendida, que sirve sólo de “contenedor” para las demás particiones. Estos sectores de arranque tienen 512 bytes de espacio para el código utilizado para arrancar un sistema operativo instalado en su partición respectiva. Esto se aplica a los sectores de arranque de particiones formateadas de DOS, Windows y OS/2, que también contienen algunos datos básicos importantes del sistema de archivos. Por el contrario, los sectores de arranque de las particiones de Linux están al principio vacíos después de configurar un sistema de archivos distinto a XFS. Por tanto, una partición de Linux no se arranca por sí misma, incluso aunque contenga un núcleo y un sistema válido de archivos raíz. Un sector de arranque con código válido para arrancar el sistema MBR tiene el mismo número mágico que el MBR en sus últimos dos bytes (`AA55`).

9.1 Selección de un cargador de arranque

Por defecto, en SUSE Linux, se utiliza el cargador de arranque GRUB. Sin embargo, en algunos casos y para configuraciones especiales de hardware y software, LILO puede ser más adecuado. Si actualiza una versión más antigua de SUSE Linux que utiliza LILO, se instala LILO.

La información relativa a la instalación y a la configuración de LILO está disponible en la base de datos de asistencia en la entrada correspondiente a la palabra clave LILO y en `/usr/share/doc/packages/lilo`.

9.2 Arranque con GRUB

GRUB (Grand Unified Boot Loader, Cargador de arranque unificado global) está dividido en dos fases: stage1 y stage2. stage1 comprende 512 bytes y su única función es cargar la segunda etapa en el cargador de arranque. Posteriormente, se carga stage2. Esta fase contiene la parte principal del cargador de arranque.

En algunas configuraciones, se puede utilizar una etapa intermedia, stage 1.5, que se encarga de localizar y cargar stage 2 desde un sistema de archivos adecuado. Si es posible, se elige este método por defecto durante la instalación o durante la configuración inicial de GRUB con YaST.

stage2 puede acceder a numerosos sistemas de archivos. Actualmente, son compatibles Ext2, Ext3, ReiserFS, Minix y el sistema de archivos DOS FAT utilizado por Windows. Hasta cierto punto, también son compatibles JFS, XFS y UFS y FFS utilizados por los sistemas BSD. A partir de la versión 0.95, GRUB también puede arrancar desde un CD o un DVD que contenga un sistema de archivos que cumpla la norma ISO 9660 de acuerdo con las especificaciones de "El Torito". Incluso antes de arrancar el sistema, GRUB puede acceder a los sistemas de archivos de dispositivos de disco de BIOS (disquetes o discos duros, unidades de CD y unidades de DVD detectados por el BIOS). Por tanto, los cambios realizados en el archivo de configuración de GRUB (`menu.lst`) no exigen que se vuelva a instalar el gestor de arranque. Cuando se arranca el sistema, GRUB vuelve a cargar el archivo del menú con las vías válidas y los datos de partición del núcleo o del disco RAM inicial (`initrd`) y ubica estos archivos.

La configuración real de GRUB está basada en tres archivos que se describen a continuación:

`/boot/grub/menu.lst`
: Este archivo contiene toda la información acerca de las particiones o de los sistemas operativos que se pueden arrancar con GRUB. Sin esta información, la línea de comandos de GRUB indica al usuario el modo de proceder (consulte "Edición de entradas de menú durante el procedimiento de arranque" (p. 218) para obtener información detallada).

`/boot/grub/device.map`
: Este archivo traduce los nombres de los dispositivos desde GRUB y la notación del BIOS a nombres de dispositivos Linux.

`/etc/grub.conf`
: Este archivo contiene los comandos, los parámetros y las opciones que necesita la shell de GRUB para instalar el cargador de arranque de forma correcta.

GRUB se puede controlar de varias maneras. Las entradas de arranque a partir de una configuración existente se pueden seleccionar en el menú gráfico (pantalla de inicio). La configuración se carga desde el archivo `menu.lst`.

En GRUB, se pueden cambiar todos los parámetros de arranque antes de arrancar. Por ejemplo, los errores cometidos al editar el archivo del menú se pueden corregir de este modo. Los comandos de arranque se pueden introducir también de forma interactiva mediante un tipo de indicador de entrada (consulte "Edición de entradas de menú durante el procedimiento de arranque" (p. 218)). GRUB ofrece la posibilidad de determinar la ubicación del núcleo y del `initrd` antes de arrancar. De este modo, puede arrancar incluso un sistema operativo instalado para el que no existe ninguna entrada en la configuración del cargador de arranque.

GRUB existe en dos versiones: como cargador de arranque y como programa normal de Linux en `/usr/sbin/grub`. Este programa, denominado *shell de GRUB,* proporciona una simulación de GRUB en el sistema instalado y se puede utilizar para instalar GRUB o probar nuevas configuraciones antes de aplicarlas. La función que permite instalar GRUB como cargador de arranque en un disco duro o en un disquete está integrada en GRUB a través de los comandos `install` y `setup`. Ésta está disponible en la shell de GRUB cuando se carga Linux.

9.2.1 Menú de arranque de GRUB

La pantalla gráfica de inicio con el menú de arranque está basada en el archivo de configuración de GRUB `/boot/grub/menu.lst`, que contiene toda la información acerca de las particiones o de los sistemas operativos que se pueden arrancar mediante el menú.

Siempre que se arranca el sistema, GRUB carga el archivo de menú a partir del sistema de archivos. Por este motivo, no es necesario volver a instalar GRUB después de efectuar cada cambio realizado al archivo. Utilice el cargador de arranque de YaST para modificar la configuración de GRUB, como se describe en la Sección 9.3, "Configuración del Cargador de arranque con YaST" (p. 222).

El archivo de menú contiene comandos. La sintaxis es muy sencilla. Todas las líneas contienen un comando seguido de parámetros opcionales separados por espacios, como en la shell. Por razones históricas, algunos comandos permiten un = delante del primer parámetro. Los comentarios se introducen con una almohadilla (#).

Para identificar los elementos del menú en la descripción general del menú, especifique una cadena `title` para cada entrada. El texto (incluidos los espacios) que sigue a la palabra `title` se muestra como opción seleccionable en el menú. Todos los comandos hasta el siguiente `title` se ejecutan cuando se selecciona este elemento del menú.

El caso más sencillo es el redireccionamiento a los cargadores de arranque de otros sistemas operativos. El comando es `chainloader` y el argumento suele ser el bloque de arranque de otra partición en la notación de bloque de GRUB. Por ejemplo:

```
chainloader (hd0,3)+1
```

Los nombres de los dispositivos de GRUB se explican en "Convenciones de nomenclatura para los discos duros y las particiones" (p. 216). Este ejemplo especifica el primer bloque de la cuarta partición del primer disco duro.

Utilice el comando `kernel` para especificar una imagen de núcleo. El primer argumento es la vía a la imagen del núcleo de una partición. Los demás argumentos se pasan a la línea de comandos del núcleo.

Si el núcleo no tiene controladores incorporados para acceder a la partición raíz, o se utiliza un sistema Linux reciente con funciones de HotPlug avanzadas, `initrd` se debe especificar con un comando de GRUB diferente cuyo único argumento es la vía al archivo `initrd`. Como la dirección de carga del `initrd` se escribe en la imagen cargada del núcleo, el comando `initrd` debe seguir inmediatamente al comando `kernel`.

El comando `root` simplifica la especificación del núcleo y de los archivos initrid. El único argumento de `root` es un dispositivo o una partición. Este dispositivo se utiliza para todos los núcleos, `initrd` y para las demás vías de archivos para las que no se especifica ningún dispositivo de forma explícita hasta el siguiente comando `root`.

El comando `boot` está implícito al final de todas las entradas de menú, de modo que no es necesario escribirlo en el archivo del menú. Sin embargo, si utiliza GRUB de forma interactiva para arrancar, debe introducir el comando `boot` al final. El comando no tiene argumentos. Sólo arranca la imagen cargada del núcleo o el cargador de cadena especificado.

Después de escribir todas las entradas de menú, defina una de ellas como entrada `default` (por defecto). De lo contrario, se utilizará la primera (entrada `0`). También es posible especificar un tiempo límite (time-out) en segundos después del cual la entrada por defecto debe arrancar. Normalmente, las entradas de menú van precedidas de `timeout` y `default`. En "Archivo de menú de ejemplo" (p. 217) se describe un archivo de ejemplo.

Convenciones de nomenclatura para los discos duros y las particiones

Las convenciones de nomenclatura que utiliza GRUB para los discos duros y las particiones son diferentes de las que se utilizan para los dispositivos normales de Linux. En GRUB, la numeración de las particiones empieza por cero. Esto significa que (`hd0,0`) es la primera partición del primer disco duro. En un equipo de escritorio estándar con un disco duro conectado como maestro principal, el nombre del dispositivo Linux correspondiente es `/dev/hda1`.

A las cuatro particiones primarias posibles se les asignan los números de partición de `0` a `3`. Las particiones lógicas se numeran a partir de `4`:

```
(hd0,0)   first primary partition of the first hard disk
(hd0,1)   second primary partition
(hd0,2)   third primary partition
(hd0,3)   fourth primary partition (usually an extended partition)
(hd0,4)   first logical partition
(hd0,5)   second logical partition
```

Dado que depende de los dispositivos del BIOS, GRUB no distingue entre dispositivos IDE, SATA, SCSI y dispositivos de hardware RAID. Todos los discos duros reconocidos por el BIOS o por otros controladores se numeran de acuerdo con la secuencia de arranque predefinida en el BIOS.

Desafortunadamente, GRUB a menudo no es capaz de asignar nombres de dispositivos Linux a nombres de dispositivos BIOS de forma exacta. Esta asignación se genera con la ayuda de un algoritmo y se guarda en el archivo `device.map`, que se puede editar si es preciso. La información relativa al archivo `device.map` está disponible en la Sección 9.2.2, “Archivo device.map” (p. 219).

Una vía completa de GRUB consiste en un nombre de dispositivo escrito entre paréntesis y la vía del archivo en el sistema de archivos de la partición especificada. La vía comienza con una barra inclinada. Por ejemplo, el núcleo arrancable se podría especificar del siguiente modo en un sistema con un único disco duro IDE que contenga Linux en la primera partición:

```
(hd0,0)/boot/vmlinuz
```

Archivo de menú de ejemplo

El siguiente ejemplo muestra la estructura de un archivo de menú GRUB. La instalación de ejemplo consta de una partición de arranque Linux en `/dev/hda5`, una partición raíz en `/dev/hda7` y una instalación de Windows en `/dev/hda1`.

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8

title linux
   kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd

title windows
   chainloader(hd0,0)+1

title floppy
   chainloader(fd0)+1

title failsafe
   kernel (hd0,4)/vmlinuz.shipped root=/dev/hda7 ide=nodma \
   apm=off acpi=off vga=normal nosmp maxcpus=0 3
   initrd (hd0,4)/initrd.shipped
```

El primer bloque define la configuración de la pantalla de inicio:

gfxmenu (hd0,4)/message
: La imagen de fondo `message` se ubica en `/dev/hda5`.

color white/blue black/light-gray
: Asignación de colores: blanco (primer plano), azul (fondo), negro (selección) y gris claro (fondo de la selección). La asignación de colores no tiene ningún efecto en la pantalla de inicio, sólo en el menú de GRUB personalizable al que es posible acceder saliendo de la pantalla de inicio con Esc.

default 0
: La primera entrada del menú `title linux` es la que se arranca por defecto.

timeout 8
: Si durante ocho segundos no se produce ninguna entrada por parte del usuario, GRUB arranca de forma automática la entrada por defecto. Para desactivar el arranque automático, elimine la línea `timeout`. Si define `timeout 0`, GRUB arranca la entrada por defecto de forma inmediata.

El segundo y mayor bloque enumera los distintos sistemas operativos que se pueden arrancar. Las secciones de cada sistema operativo se introducen por `title`.

- La primera entrada (`title linux`) se encarga de arrancar SUSE Linux. El núcleo (`vmlinuz`) se ubica en la primera partición lógica (partición de arranque) del primer disco duro. Los parámetros del núcleo, como la partición raíz y el modo VGA, se añaden aquí. La partición raíz se especifica según la convención de nomenclatura de Linux (`/dev/hda7/`), porque esta información se lee por el núcleo y no tiene nada que ver con GRUB. El `initrd` también se ubica en la primera partición lógica del primer disco duro.

- La segunda entrada se encarga de cargar Windows. Windows se arranca desde la primera partición del primer disco duro (`hd0,0`). El comando `chainloader +1` hace que GRUB lea y ejecute el primer sector de la partición especificada.

- La siguiente entrada habilita el arranque desde el disquete sin modificar la configuración del BIOS.

- La opción de arranque `failsafe` arranca Linux con una selección de parámetros de núcleo que habilita Linux para arrancar incluso en sistemas que presenten problemas.

El archivo del menú se puede cambiar siempre que sea necesario. Durante el siguiente arranque, GRUB utilizará la configuración modificada. Edite el archivo de forma permanente mediante YaST o mediante el editor que prefiera. Como alternativa, realice cambios temporales de forma interactiva mediante la función de edición de GRUB. Consulte "Edición de entradas de menú durante el procedimiento de arranque" (p. 218).

Edición de entradas de menú durante el procedimiento de arranque

En el menú de arranque gráfico de GRUB, seleccione el sistema operativo para el arranque con las teclas de flecha. Si selecciona un sistema Linux, puede introducir parámetros de arranque adicionales en el indicador de inicio. Para editar entradas de menú por separado directamente, pulse Esc para salir de la pantalla de inicio y acceder al menú de texto de GRUB y, a continuación, pulse E. Los cambios realizados de este modo sólo se aplican al procedimiento de arranque en curso, no se adoptan de forma permanente.

IMPORTANTE: Distribución del teclado durante el procedimiento de arranque

La distribución del teclado americano es la única disponible al arrancar.

La edición de entradas del menú facilita la reparación de un sistema defectuoso que no se puede arrancar, dado que el archivo de configuración defectuoso del cargador de arranque se puede eludir introduciendo los parámetros de forma manual. La introducción de los parámetros de forma manual durante el procedimiento de arranque también es útil para probar la configuración nueva sin dañar el sistema original.

Después de activar el modo de edición, utilice las teclas de flecha para seleccionar la entrada del menú cuya configuración quiera editar. Para que la configuración sea editable, pulse E una vez más. De este modo, edite las particiones incorrectas o las especificaciones de vías antes de que tengan un efecto negativo en el proceso de arranque. Pulse Intro para salir del modo de edición y volver al menú. A continuación, pulse B para arrancar esta entrada. Las acciones que se pueden llevar a cabo a continuación se muestran en el texto de ayuda que aparece al final.

Para introducir las opciones de arranque cambiadas de forma permanente y pasarlas al núcleo, abra `menu.lst` como usuario `root` y añada los parámetros respectivos del núcleo a la línea existente, separados por espacios:

```
title linux
   kernel (hd0,0)/vmlinuz root=/dev/hda3 additional parameter
   initrd (hd0,0)/initrd
```

La siguiente vez que se arranca el sistema, GRUB adopta de forma automática los parámetros nuevos. Como alternativa, este cambio también se puede realizar con el módulo del cargador de arranque YaST. Añada los parámetros nuevos a la línea existente, separados por espacios.

9.2.2 Archivo device.map

El archivo `device.map` asigna nombres de dispositivos de GRUB y del BIOS a los nombres de dispositivos Linux. En un sistema mixto que contenga discos duros IDE y SCSI, GRUB debe tratar de determinar la secuencia de arranque mediante un procedimiento especial, ya que GRUB no tiene acceso a la información del BIOS de la secuencia de arranque. GRUB guarda el resultado de este análisis en el archivo `/boot/grub/device.map`. Para un sistema en el que la secuencia de arranque del BIOS se define

como IDE antes de SCSI, el archivo `device.map` podría aparecer de la siguiente forma:

```
(fd0)  /dev/fd0
(hd0)  /dev/hda
(hd1)  /dev/sda
```

Como el orden de IDE, SCSI y los demás discos duros dependen de varios factores y Linux no es capaz de identificar la asignación, la secuencia del archivo `device.map` se puede definir de forma manual. Si encuentra problemas al arrancar, compruebe si la secuencia de este archivo corresponde a la secuencia del BIOS y utilice el indicador de GRUB para modificarlo de forma temporal si es preciso. Una vez que el sistema Linux ha arrancado, el archivo `device.map` se puede editar de forma permanente con el módulo del cargador de arranque YaST o con el editor que desee.

IMPORTANTE: Discos SATA

Según el controlador, los discos SATA se reconocen como dispositivos IDE (/dev/hd*x*) o SCSI (/dev/sd*x*).

Después de cambiar de forma manual `device.map`, ejecute el siguiente comando para volver a instalar GRUB. Este comando hace que el archivo `device.map` se vuelva a cargar y que los comandos escuchados en `grub.conf` se ejecuten:

```
grub --batch < /etc/grub.conf
```

9.2.3 Archivo /etc/grub.conf

El tercer archivo de configuración de GRUB más importante, después de `menu.lst` y `device.map`, es `/etc/grub.conf`. Este archivo contiene los comandos, los parámetros y las opciones que necesita la shell de GRUB para instalar el cargador de arranque de forma correcta:

```
root (hd0,4)
   install /grub/stage1 (hd0,3) /grub/stage2 0x8000 (hd0,4)/grub/menu.lst
   quit
```

Significado de las entradas individuales:

root (hd0,4)
: Este comando le dice a GRUB que aplique los siguientes comandos a la primera partición lógica del primer disco duro (la ubicación de los archivos de arranque).

`parámetro` install

El comando `grub` debe ejecutarse con el parámetro `install`. `stage1` del cargador de arranque debe instalarse en el contenedor de la partición extendida (`/grub/stage1 d (hd0,3)`). `stage2` debe cargarse en la dirección de memoria 0x8000 (`/grub/stage2 0x8000`). La última entrada (`(hd0,4)/grub/menu.lst`) le dice a GRUB dónde buscar el archivo del menú.

9.2.4 Configuración de una contraseña de arranque

Incluso antes de que se arranque el sistema operativo, GRUB habilita el acceso a los sistemas de archivos. Los usuarios sin permisos root pueden acceder a los archivos del sistema Linux a los que no tienen acceso una vez arrancado el sistema. Para bloquear este tipo de acceso o impedir que los usuarios arranquen ciertos sistemas operativos, defina una contraseña de arranque.

IMPORTANTE: Contraseña de arranque y pantalla de inicio

Si utiliza una contraseña de inicio para GRUB, no se muestra la pantalla de inicio habitual.

Como usuario `root`, realice lo siguiente para definir una contraseña de arranque:

1. En el indicador de root, introduzca `grub`.

2. Cifre la contraseña en la shell del GRUB:

```
grub> md5crypt
Password: ****
Encrypted: $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

3. Pegue la cadena cifrada en la sección global del archivo `menu.lst`:

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8
password --md5 $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

Ahora los comandos GRUB sólo se pueden ejecutar en el indicador de inicio después de pulsar P e introducir la contraseña. Sin embargo, los usuarios aún pueden arrancar los sistemas operativos desde el menú de arranque.

4 Para evitar que uno o varios sistemas operativos se arranquen desde el menú de arranque, añada la entrada `lock` a todas las secciones de `menu.lst` que no deberían poder arrancarse sin introducir una contraseña. Por ejemplo:

```
title linux
   kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd
   lock
```

Después de volver a arrancar el sistema y seleccionar la entrada Linux en el menú de arranque, aparece el siguiente mensaje de error:

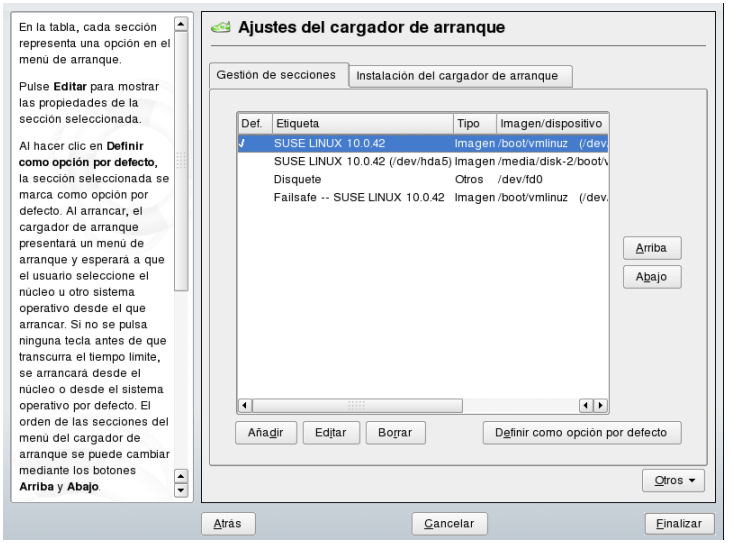
```
Error 32: Debe autenticarse
```

Pulse Intro para entrar en el menú. A continuación, pulse P para obtener un indicador de contraseña. Después de introducir la contraseña y pulsar Intro, debería arrancarse el sistema operativo seleccionado (en este caso, Linux).

9.3 Configuración del Cargador de arranque con YaST

La forma más sencilla de configurar el cargador de arranque en el sistema SUSE Linux es mediante el módulo YaST. En el Centro de control de YaST, seleccione *Sistema* → *Configuración del cargador de arranque.* Como en la Figura 9.1, “Configuración del Cargador de arranque con YaST” (p. 223), se muestra así la configuración en uso del cargador de arranque en el sistema y es posible hacer cambios.

Figura 9.1 *Configuración del Cargador de arranque con YaST*



Utilice la pestaña *Gestión de sesiones* para editar, cambiar y suprimir las secciones del cargador de arranque correspondientes a los sistemas operativos individuales. Para añadir una opción, haga clic en *Añadir*. Para cambiar el valor de una opción existente, selecciónelo con el ratón y haga clic en *Editar*. Si no quiere utilizar una opción existente, selecciónela y haga clic en *Suprimir.* Si no está familiarizado con las opciones del cargador de arranque, lea antes la Sección 9.2, “Arranque con GRUB” (p. 212).

Utilice la pestaña *Instalación del cargador de arranque* para ver y cambiar los ajustes relacionados con el tipo, la ubicación y las opciones avanzadas del cargador.

9.3.1 Tipo del cargador de arranque

Defina el tipo de cargador de arranque en *Instalación del cargador de arranque.* GRUB es, por defecto, el cargador de arranque que se utiliza en SUSE Linux. Para usar LILO, siga los pasos que se especifican a continuación:

Procedimiento 9.1 *Cambio del tipo de cargador de arranque*

1 Seleccione la pestaña *Instalación del cargador de arranque.*

2 En *Cargador de arranque,* seleccione *LILO.*

3 En el cuadro de diálogo que se abre, seleccione una de las acciones siguientes:

Proponer nueva configuración
: Hace que YaST proponga una configuración nueva.

Convertir la configuración actual
: Hace que YaST convierta la configuración en uso. Algunos ajustes pueden perderse al convertir la configuración.

Iniciar nueva configuración desde cero
: Escriba una configuración personalizada. Esta acción no se encuentra disponible durante la instalación de SUSE Linux.

Cargar la configuración guardada en el disco
: Se carga un archivo `/etc/lilo.conf` propio. Esta acción no se encuentra disponible durante la instalación de SUSE Linux.

4 Haga clic en *Aceptar* para guardar los cambios

5 Haga clic en *Finalizar* en el cuadro de diálogo principal para aplicar los cambios.

Tras efectuar la conversión, la configuración de GRUB anterior se guarda en el disco. Para utilizarla, basta con cambiar el tipo de cargador de arranque a GRUB y elegir *Restablecer configuración guardada antes de la conversión.* Esta acción está disponible únicamente en un sistema instalado.

NOTA: Cargador de arranque personalizado

Si desea utilizar un cargador de arranque distinto a GRUB o LILO, seleccione *No instalar ningún cargador de arranque.* Lea con atención la documentación del cargador de arranque antes de seleccionar esta opción.

9.3.2 Ubicación del cargador de arranque

Para cambiar la ubicación del cargador de arranque, siga estos pasos:

Procedimiento 9.2 *Cambio de la ubicación del cargador de arranque*

1. Seleccione la pestaña *Instalación del cargador de arranque* y después elija una de las opciones siguientes en *Ubicación del cargador de arranque:*

   Registro de inicio principal de /dev/hdX
   : Con esta opción se instala el cargador de arranque en el MBR de un disco. X identifica el disco duro, por ejemplo, a, b, c o d:

     ```
     hda => ide0 master
     hdb => ide0 slave
     hdc => ide1 master
     hdd => ide1 slave
     ```

   Sector de arranque de la partición de arranque /dev/hdXY
   : El sector de arranque de la partición `/boot`. Esta opción se establece por defecto si se dispone de varios sistemas operativos instalados en el disco duro. Y corresponde a la partición (1, 2, 3, 4, 5, etc.), como en:

     ```
     /dev/hda1
     ```

   Sector de arranque de la partición raíz /dev/hdXY
   : El sector de arranque de la partición (raíz) `/`. A menos que sea necesaria una partición `/boot` o que se deba usar el MBR, éste es el valor por defecto preferible.

   Other (Otros)
   : Esta opción permite especificar la ubicación del cargador de arranque manualmente.

2. Haga clic en *Finalizar* para aplicar los cambios.

9.3.3 Sistema por defecto

Para cambiar el sistema que se arranca por defecto, haga lo siguiente:

Procedimiento 9.3 *Configuración del sistema por defecto*

1. Abra la pestaña *Gestión de secciones.*

2. Seleccione el sistema que desee de la lista.

3 Haga clic en *Definir como opción por defecto*.

4 Haga clic en *Finalizar* para hacer efectivos los cambios.

9.3.4 Tiempo límite del cargador de arranque

El cargador de arranque no inicia el sistema por defecto de forma inmediata. Durante el tiempo límite, puede seleccionar que el sistema arranque, o bien escribir algunos parámetros del núcleo. Para aumentar o disminuir el tiempo límite del cargador de arranque, siga los pasos que se especifican a continuación:

Procedimiento 9.4 *Cambio del tiempo límite del cargador de arranque*

1 Abra la pestaña *Instalación del cargador de arranque.*

2 Haga clic en *Opciones del cargador de arranque*.

3 Marque *Modo de arranque*.

4 En *Menú de arranque,* cambie el valor de *Tiempo límite de menú de arranque* escribiendo un nuevo valor, haciendo clic con el ratón en la flecha apropiada o utilizando las teclas de flecha del teclado.

5 Haga clic en *Aceptar*.

6 Haga clic en *Finalizar* para guardar los cambios.

Puede definir que el menú de arranque se muestre de forma permanente sin tiempo límite inhabilitando la opción *Continuar arranque tras tiempo de espera.*

9.3.5 Ajustes de seguridad

También puede utilizar este módulo YaST para definir una contraseña con la que proteger el arranque. Con esto, se alcanza un nivel superior de seguridad.

Procedimiento 9.5 *Definición de una contraseña para el cargador de arranque*

1. Abra la pestaña *Instalación del cargador de arranque.*
2. Haga clic en *Opciones del cargador de arranque*.
3. En *Protección mediante contraseña,* marque *Proteger el cargador de arranque mediante contraseña* y defina la contraseña.
4. Haga clic en *Aceptar*.
5. Haga clic en *Finalizar* para guardar los cambios.

9.3.6 Orden de los discos

Si su equipo tiene más de un disco duro, puede especificar la secuencia de arranque de los discos para que coincida con la configuración del BIOS de la máquina (consulte la Sección 9.2.2, “Archivo device.map” (p. 219)). Para ello, siga los pasos que se especifican a continuación:

Procedimiento 9.6 *Configuración del orden de los discos*

1. Abra la pestaña *Instalación del cargador de arranque.*
2. Haga clic en *Detalles de la instalación del cargador de arranque*.
3. Si aparecen varios discos duros, seleccione uno de ellos y haga clic en *Arriba* o *Abajo.*
4. Haga clic en *Aceptar* para guardar los cambios.
5. Haga clic en *Finalizar* para guardar los cambios.

También puede utilizar este módulo para sustituir el registro de arranque principal con código genérico para arrancar la partición activa. Haga clic en *Sustituir MBR por código genérico* en *Actualización del área del sistema del disco.* Habilite *Activar la partición del cargador de arranque* para activar la partición que contiene el cargador de arranque. Haga clic en *Finalizar* para guardar los cambios.

9.4 Desinstalación del cargador de arranque de Linux

YaST se puede utilizar para desinstalar el cargador de arranque de Linux y restaurar el estado que el MBR tenía antes de instalar Linux. Durante la instalación, YaST crea de forma automática una copia de seguridad del MBR original y lo restaura cuando se le solicita.

Para desinstalar GRUB, inicie el módulo del cargador de arranque de YaST (*Sistema → Configuración del cargador de arranque*). En el primer cuadro de diálogo, seleccione *Reset → Restore MBR of Hard Disk* (Restablecer - Restablecer MBR de disco duro) y salga del cuadro de diálogo mediante *Finalizar*.

9.5 Creación de CD de arranque

Si se producen problemas al arrancar el sistema mediante un gestor de arranque, o si éste no se puede instalar en el MBR del disco duro o disquete, es posible crear un CD de arranque que incluya todos los archivos de inicio necesarios para Linux. Para ello, es preciso tener instalada en el sistema una grabadora de CD.

Para crear un CD-ROM de arranque con GRUB, sólo es necesario una variante especial de *stage2,* llamada `stage2_eltorito` y, si se desea, un archivo `menu.lst` personalizado. No son necesarios los archivos `stage1` y `stage2` habituales.

Procedimiento 9.7 *Creación de CD de arranque*

1. Cree un directorio en el que se deba crear la imagen ISO, por ejemplo:

   ```
   cd /tmp
   mkdir iso
   ```

2. Cree un subdirectorio para GRUB:

   ```
   mkdir -p iso/boot/grub
   ```

3. Copie el núcleo, los archivos `stage2_eltorito`, `initrd` y `menu.lst`, así como `/boot/message` a `iso/boot/`:

```
cp /boot/vmlinuz iso/boot/
cp /boot/initrd iso/boot/
cp /boot/message iso/boot/
cp /boot/grub/menu.lst iso/boot/grub
```

4 Ajuste las entradas de vía de `iso/boot/menu.lst` para que señalen a un dispositivo de CD-ROM. Para ello, se debe reemplazar el nombre de dispositivo de los discos duros, que se muestran con el formato `(hd*)`, en los nombres de vías con el nombre de dispositivo de la unidad de CD-ROM, es decir, `(cd)`:

```
gfxmenu (cd)/boot/message
timeout 8
default 0

title Linux
   kernel (cd)/boot/vmlinuz root=/dev/hda5 vga=794 resume=/dev/hda1 \
   splash=verbose showopts
   initrd (cd)/boot/initrd
```

5 Cree la imagen ISO con el comando siguiente:

```
mkisofs -R -b boot/grub/stage2_eltorito -no-emul-boot \
-boot-load-size 4 -boot-info-table -o grub.iso iso
```

6 Copie el archivo resultante, `grub.iso`, a un CD con la utilidad que prefiera.

9.6 Pantalla gráfica de SUSE

A partir de SUSE Linux 7.2, la pantalla gráfica de SUSE se muestra en la primera consola si la opción “vga=<value>” se utiliza como parámetro del núcleo. Si lleva a cabo la instalación mediante YaST, esta opción se activa de forma automática de acuerdo con la resolución seleccionada y con la tarjeta gráfica. Hay tres modos de inhabilitar la pantalla de SUSE, si se desea:

Inhabilitación de la pantalla de SUSE en caso necesario.
: Introduzca el comando `echo 0 >/proc/splash` en la línea de comandos para inhabilitar la pantalla gráfica. Para volver a activarla, introduzca `echo 1 >/proc/splash`.

Inhabilitación de la pantalla de SUSE por defecto.
: Añada el parámetro del núcleo `splash=0` a la configuración del cargador de arranque. El Capítulo 9, *Cargador de arranque* (p. 211) proporciona más información

acerca de esto. Sin embargo, si prefiere el modo de texto, que era el modo por defecto en versiones anteriores, defina `vga=normal`.

Inhabilitación completa de la pantalla de SUSE.
: Recopile un núcleo nuevo e inhabilite la opción *Use splash screen instead of boot logo* (Utilizar la pantalla de inicio en lugar del logotipo de arranque) en *framebuffer support* (asistencia de framebuffer).

SUGERENCIA

Si se inhabilita la asistencia de framebuffer en el núcleo, también se inhabilita de forma automática la pantalla de inicio. Si ejecuta el sistema con un núcleo personalizado, SUSE no proporciona asistencia.

9.7 Solución de problemas

En esta sección se enumeran algunos de los problemas que se encuentran habitualmente al arrancar con GRUB y una descripción breve de las posibles soluciones. Algunos de los problemas se tratan en artículos de la base de datos de asistencia en `http://portal.suse.de/sdb/en/index.html`. Si su problema en concreto no aparece en esta lista, utilice el cuadro de búsqueda de la base de datos de asistencia de `https://portal.suse.com/PM/page/search.pm` para buscar palabras clave como *GRUB*, *arrancar* y *cargador de arranque*.

GRUB y XFS
: XFS no deja espacio para `stage1` en el bloque de arranque de la partición. Por tanto, no especifique una partición de XFS como ubicación del cargador de arranque. Este problema se puede solucionar creando una partición de arranque separada que no se formatea con XFS.

GRUB y JFS
: Aunque técnicamente es posible, la combinación de GRUB con JFS presenta problemas. En este caso, cree una partición de arranque separada (`/boot`) y formatéela con Ext2. Instale GRUB en esta partición.

GRUB informa de un error de geometría
: GRUB comprueba la geometría de los discos duros conectados cuando se arranca el sistema. Algunas veces, el BIOS devuelve información no coherente y GRUB

informa de un error de geometría de GRUB. En este caso, utilice LILO o actualice el BIOS. La información detallada acerca de la instalación, de la configuración y del mantenimiento de LILO está disponible en la base de datos de asistencia si se busca con la palabra clave LILO.

GRUB también devuelve este mensaje de error si Linux se instaló en un disco duro adicional no registrado en el BIOS. *stage1* del cargador de arranque se encuentra y se carga de forma correcta, pero *stage2* no se encuentra. Este problema se puede solucionar registrando el disco duro nuevo en el BIOS.

El sistema que contiene los discos duros IDE y SCSI no arranca
: Durante la instalación, puede que YaST haya determinado la secuencia de arranque de los discos duros de forma incorrecta. Por ejemplo, GRUB puede considerar `/dev/hda` as `hd0` y `/dev/sda` como `hd1`, aunque la secuencia de arranque del BIOS esté invertida (SCSI *antes de* IDE).

  En este caso, corrija los discos duros durante el proceso de arranque con la ayuda de la línea de comandos de GRUB. Una vez que el sistema haya arrancado, edite el archivo `device.map` para aplicar la nueva asignación de forma permanente. A continuación, busque los nombres de dispositivos de GRUB en los archivos`/boot/grub/menu.lst` y `/boot/grub/device.map` y vuelva a instalar el cargador de arranque con el siguiente comando:

  ```
  grub --batch < /etc/grub.conf
  ```

Arranque de Windows desde el segundo disco duro
: Algunos sistemas operativos, como Windows, sólo pueden arrancar desde el primer disco duro. Si uno de esos sistemas operativos está instalado en un disco duro que no sea el primero, puede llevar a cabo un cambio lógico en la entrada de menú respectiva.

  ```
  ...
  title windows
     map (hd0) (hd1)
     map (hd1) (hd0)
     chainloader(hd1,0)+1
  ...
  ```

  En este ejemplo, Windows se inicia desde el segundo disco duro. Para ello, el orden lógico de los discos duros se cambia con `map`. Este cambio no afecta a la lógica del archivo del menú de GRUB. Por tanto, el segundo disco duro se debe especificar con `chainloader`.

9.8 Información adicional

La información detallada acerca de GRUB se encuentra disponible en `http://www.gnu.org/software/grub/`. Consulte también la página de información de `grub`. También puede buscar la palabra clave “GRUB” en la base de datos de asistencia en `http://portal.suse.de/sdb/en/index.html` para obtener información acerca de asuntos especiales.

10 Funciones especiales de SUSE Linux

Este capítulo incluye información acerca de varios paquetes de software, las consolas virtuales y el formato del teclado. Se describen componentes de software como, por ejemplo, `bash`, `cron`, y `logrotate`, ya que han experimentado mejoras o cambios en las últimas versiones. Aunque dichos cambios sean pequeños o tengan una importancia menor, es posible que los usuarios deseen cambiar su comportamiento por defecto, ya que estos componentes están a menudo muy vinculados al sistema. El capítulo finaliza con un apartado sobre los ajustes regionales y de idioma (I18N y L10N).

10.1 Información acerca de paquetes especiales de software

Los programas `bash`, `cron`, `logrotate`, `locate`, `ulimit` y `free`, así como el archivo `resolv.conf`, revisten gran importancia, tanto para los administradores de los sistemas como para muchos usuarios. Las páginas de manual (Man) y las de información (Info) constituyen dos útiles fuentes de información sobre comandos, si bien a veces no están las dos disponibles. GNU Emacs es un editor de texto muy utilizado y con muchas opciones de configuración.

10.1.1 Paquete bash y /etc/profile

Bash es la shell por defecto de SUSE Linux. Cuando se utiliza como shell de inicio de sesión, lee varios archivos de inicialización y los procesa en el orden en el que aparecen en la lista.

1. `/etc/profile`
2. `~/.profile`
3. `/etc/bash.bashrc`
4. `~/.bashrc`

En `~/.profile` y en `~/.bashrc` se pueden aplicar ajustes personalizados. Para garantizar que estos archivos se procesen correctamente, es necesario copiar los ajustes básicos desde `/etc/skel/.profile` o `/etc/skel/.bashrc` en el directorio personal del usuario. Se recomienda copiar los ajustes de `/etc/skel` tras una actualización. Ejecute los siguientes comandos shell para evitar que se pierdan ajustes personales:

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

A continuación, copie los ajustes personales otra vez de los archivos `*.old`.

10.1.2 Paquete cron

Si desea ejecutar comandos de forma regular y automática en segundo plano a horas predefinidas, cron es la herramienta tradicional que utilizar. Funciona mediante tablas horarias con un formato especial para ello. Algunas de estas tablas acompañan al sistema y, si así lo desean o si es necesario, los usuarios pueden escribir sus propias tablas.

Las tablas cron se encuentran en `/var/spool/cron/tabs`. `/etc/crontab` sirve como tabla cron para todo el sistema. Escriba el nombre de usuario para ejecutar el comando directamente después de la tabla horaria y antes del comando. En el Ejemplo 10.1, “Entrada en /etc/crontab” (p. 234), se ha introducido `Root`. Las tablas específicas del paquete, ubicadas en `/etc/cron.d`, comparten el mismo formato. Consulte la página Man sobre `cron` (`man cron`).

Ejemplo 10.1 *Entrada en /etc/crontab*

```
1-59/5 * * * *   root   test -x /usr/sbin/atrun && /usr/sbin/atrun
```

No es posible editar `/etc/crontab` ejecutando el comando `crontab -e`. Este archivo se debe cargar directamente en un editor, después modificarse y finalmente guardarse.

Hay varios paquetes que instalan guiones shell en los directorios `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` y `/etc/cron.monthly`, cuya ejecución se controla a través de `/usr/lib/cron/run-crons`. `/usr/lib/cron/run-crons` se ejecuta cada 15 minutos desde la tabla principal (`/etc/crontab`). Esto garantiza que los procesos que se hayan podido descuidar puedan ejecutarse en el momento adecuado.

Para ejecutar los guiones `hourly` (cada hora), `daily` (cada día), u otros guiones de mantenimiento periódicos en momentos personalizados, elimine los archivos de marca horaria de forma regular mediante entradas `/etc/crontab`. Consulte el Ejemplo 10.2, "/etc/crontab: eliminación de archivos de marca horaria" (p. 235), donde se elimina el guión `hourly` (cada hora) antes de cada hora en punto y el guión `daily` (cada día) una vez al día a las 2:14 a.m., etc.

Ejemplo 10.2 *`/etc/crontab`: eliminación de archivos de marca horaria*

```
59 *  * * *     root  rm -f /var/spool/cron/lastrun/cron.hourly
14 2  * * *     root  rm -f /var/spool/cron/lastrun/cron.daily
29 2  * * 6     root  rm -f /var/spool/cron/lastrun/cron.weekly
44 2  1 * *     root  rm -f /var/spool/cron/lastrun/cron.monthly
```

Los trabajos de mantenimiento del sistema diarios se han distribuido entre varios guiones para conseguir una mayor claridad. Estos trabajos están dentro del paquete `aaa_base`. `/etc/cron.daily` contiene, por ejemplo, los componentes `suse.de-backup-rpmdb`, `suse.de-clean-tmp` o `suse.de-cron-local`.

10.1.3 Archivos de registro: paquete logrotate

Ciertos servicios del sistema *(daemons),* junto con el núcleo en sí, registran en archivos de registro y de forma regular el estado del sistema y eventos concretos. Así, el administrador puede comprobar con regularidad el estado del sistema en un momento concreto, reconocer errores o funciones defectuosas y repararlos con precisión. Estos archivos de registro generalmente se almacenan en `/var/log`, tal y como especifica el estándar FHS, y van creciendo cada día. El paquete `logrotate` ayuda a controlar el crecimiento de estos archivos.

Configure logrotate con el archivo `/etc/logrotate.conf`. En concreto, la especificación `include` (incluir) configura principalmente los archivos adicionales que se deben leer. SUSE Linux garantizará que los programas que generan archivos de registro instalen archivos de configuración individuales en `/etc/logrotate.d`. Por ejemplo, estos programas incluyen los paquetes `apache2` (`/etc/logrotate.d/apache2`) y `syslogd` (`/etc/logrotate.d/syslog`).

Ejemplo 10.3 *Ejemplo para /etc/logrotate.conf*

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#    monthly
#    create 0664 root utmp
#    rotate 1
#}

# system-specific logs may be also be configured here.
```

logrotate se controla mediante cron y se ejecuta a diario a través de `/etc/cron.daily/logrotate`.

IMPORTANTE

La opción `create` (crear) lee todos los ajustes realizados por el administrador en `/etc/permissions*`. Asegúrese de que no se produzcan conflictos a raíz de posibles modificaciones personales.

10.1.4 Comando locate

El comando locate, que permite buscar archivos de forma rápida, no está incluido en el ámbito estándar del software instalado. Si lo desea, instale el paquete `find-locate`. El proceso updatedb se inicia automáticamente cada noche o alrededor de 15 minutos después de iniciar el sistema.

10.1.5 Comando ulimit

El comando `ulimit` *(límites de usuario)* permite definir límites para el uso de recursos del sistema, así como para que se puedan mostrar estos recursos. El comando `ulimit` resulta especialmente útil para limitar la memoria disponible para las distintas aplicaciones. Con este comando se puede hacer que una aplicación no utilice demasiada memoria por sí sola, una situación que podría detener el sistema.

`ulimit` se puede utilizar con varias opciones. Para limitar el uso de memoria, utilice las opciones que se muestran en la Tabla 10.1, “`ulimit`: definición de recursos para el usuario” (p. 237).

Tabla 10.1 *ulimit: definición de recursos para el usuario*

`-m`	Tamaño máximo de memoria física
`-v`	Tamaño máximo de memoria virtual
`-s`	Tamaño máximo del stack
`-c`	Tamaño máximo de los archivos de núcleo central
`-a`	Visualización de límites

En `/etc/profile` se pueden definir entradas para todo el sistema. Habilite aquí la creación de archivos de núcleo central que necesitan los programadores para poder realizar operaciones de *depuración.* Un usuario normal no puede aumentar los valores que haya especificado el administrador del sistema en `/etc/profile`, pero puede crear entradas especiales en `~/.bashrc`.

Ejemplo 10.4 *ulimit: ajustes en ~/.bashrc*

```
# Limits of physical memory:
ulimit -m 98304

# Limits of virtual memory:
ulimit -v 98304
```

La cantidad de memoria se debe especificar en KB. Para obtener más información, consulte `man bash`.

IMPORTANTE

No todas las shells admiten las directivas `ulimit`. PAM (por ejemplo `pam_limits`) ofrece un completo elenco de posibilidades de ajuste en caso de que se deban abarcar ajustes para estas restricciones.

10.1.6 Comando free

El comando `free` resulta en cierta manera engañoso si el objetivo es saber cuánta memoria RAM se está utilizando en esos momentos. Esa información se puede consultar en `/proc/meminfo`. En la actualidad, los usuarios con acceso a un sistema operativo moderno, como Linux, no deberían necesitar preocuparse demasiado sobre el uso de memoria. El concepto de *RAM disponible* se remonta a los días anteriores a la gestión de la memoria unificada. La frase *memoria libre es memoria mala* se aplica también en Linux. Así, Linux se ha esforzado siempre en equilibrar las cachés sin permitir que haya memoria libre o no utilizada.

Básicamente, el núcleo no tiene conocimiento directo de ninguna aplicación ni de ningún dato del usuario, sino que gestiona las aplicaciones y los datos del usuario en una *caché de páginas.* Si la memoria se queda corta, se escriben partes de ella en la partición de intercambio o en archivos desde los cuales se podrá leer con ayuda del comando `mmap` (consulte `man mmap`).

El núcleo también contiene otras cachés, como la *caché de tablas,* donde se almacenan la cachés utilizadas para acceder a la red. Esto puede explicar las diferencias entre los contadores en `/proc/meminfo`. A la mayoría de ellas, pero no a todas, se puede acceder a través de `/proc/slabinfo`.

10.1.7 Archivo /etc/resolv.conf

La resolución del nombre de dominio se gestiona a través del archivo `/etc/resolv.conf`. Consulte el Capítulo 20, *Sistema de nombres de dominio (DNS)* (p. 397).

Este archivo se actualiza con el guión `/sbin/modify_resolvconf` de forma exclusiva, ningún otro programa dispone de permiso para modificar `/etc/resolv.conf` directamente. Aplicar esta regla es la única manera de garantizar que la configuración de red del sistema y los archivos relevantes se guardan en un estado coherente.

10.1.8 Páginas Man y páginas Info

Para algunas aplicaciones de GNU (como tar), las páginas Man correspondientes han dejado de publicarse. Para estos comandos, utilice la opción `--help` y obtendrá una descripción general de las páginas Info, las cuales proporcionan instrucciones más detalladas a través del sistema de hipertexto de GNU. Lea una introducción a este sistema escribiendo `info info`. Las páginas Info se pueden ver con Emacs escribiendo `emacs -f info`, o directamente en una consola con `info`. También podrá ver páginas Info con tkinfo, xinfo o el sistema de ayuda de SUSE.

10.1.9 Ajustes para GNU Emacs

GNU Emacs es un entorno de trabajo complejo. En las siguientes secciones se describen los archivos de configuración que se procesan al iniciar GNU Emacs. Encontrará más información en `http://www.gnu.org/software/emacs/`.

Al iniciarse, Emacs lee varios archivos que contienen los ajustes para el usuario, el administrador del sistema y el distribuidor de personalización o configuración previa. El archivo de inicio `~/.emacs` se instala en los directorios personales de cada usuario desde `/etc/skel`. `.emacs`, a su vez, lee el archivo `/etc/skel/.gnu-emacs`. Para personalizar el programa, copie `.gnu-emacs` en el directorio personal (con `cp /etc/skel/.gnu-emacs ~/.gnu-emacs`) y aplique allí los ajustes que desee.

`.gnu-emacs` define el archivo `~/.gnu-emacs-custom` como `custom-file` (archivo personalizado). Si el usuario desea efectuar ajustes con las opciones `customize` (personalizar) en Emacs, dichos ajustes se guardarán en `~/.gnu-emacs-custom`.

Con SUSE Linux, el paquete `emacs` instala el archivo `site-start.el` en el directorio `/usr/share/emacs/site-lisp`. El archivo `site-start.el` se carga antes que el archivo de inicio `~/.emacs`. Entre otros aspectos, `site-start.el` se ocupa de que los archivos de configuración distribuidos con los paquetes complementarios de Emacs como, por ejemplo, `psgml`, se carguen automáticamente. Tales archivos de configuración se encuentran también en `/usr/share/emacs/site-lisp` y comienzan siempre con `suse-start-`. El administrador local del sistema puede definir ajustes de configuración válidos para todo el sistema con `default.el`.

Encontrará más información acerca de estos archivos en el archivo de información de Emacs en *Init File*: `info:/emacs/InitFile`. Aquí también encontrará información acerca de cómo evitar la carga de estos archivos cuando sea necesario.

Los componentes de Emacs están distribuidos en varios paquetes:

- Paquete básico `emacs`.
- `emacs-x11`: se instala normalmente e *incluye* compatibilidad con X11.
- `emacs-nox`: programa *sin* compatibilidad con X11.
- `emacs-info`: documentación en línea en formato info.
- `emacs-el`: contiene archivos de bibliotecas sin compilar en Emacs Lisp. No son necesarios para el tiempo de ejecución.
- Se pueden instalar numerosos paquetes complementarios si es necesario: `emacs-auctex` (para LaTeX), `psgml` (para SGML y XML), `gnuserv` (para el uso del cliente y el servidor), etc.

10.2 Consolas virtuales

Linux es un sistema multiusuario y multitarea. Las ventajas que presentan estas características se pueden apreciar incluso en un sistema autónomo. El modo de texto presenta seis consolas virtuales. Cambie de una a otra pulsando las combinaciones de teclas de Alt + F1 a Alt + F6. La séptima consola se reserva para X, y la décima muestra los mensajes del núcleo. Se podrán asignar más o menos consolas modificando el archivo `/etc/inittab`.

Para cambiar a una consola desde X sin cerrar, utilice las combinaciones de teclas de Ctrl + Alt + F1 a Ctrl + Alt + F6. Para volver a X, pulse Alt + F7.

10.3 Distribución del teclado

Para estandarizar la distribución del teclado de los distintos los programas, se han hecho cambios en los siguientes archivos:

```
/etc/inputrc
/usr/X11R6/lib/X11/Xmodmap
/etc/skel/.Xmodmap
/etc/skel/.exrc
/etc/skel/.less
/etc/skel/.lesskey
/etc/csh.cshrc
/etc/termcap
/usr/lib/terminfo/x/xterm
/usr/X11R6/lib/X11/app-defaults/XTerm
/usr/share/emacs/<VERSION>/site-lisp/term/*.el
```

Estas modificaciones sólo tienen efecto sobre aplicaciones que usan las entradas `terminfo` o cuyos archivos de configuración se modificaron directamente (`vi`, `less`, etc.). Se recomienda adaptar otras aplicaciones que no sean de SUSE Linux a estas definiciones por defecto.

En el entorno X, se puede acceder a la tecla Compose (tecla compuesta) mediante la combinación de teclas Ctrl + Mayús (derecha). También puede consultar la entrada correspondiente en `/usr/X11R6/lib/X11/Xmodmap`.

X Keyboard Extension (XKB) permite acceder a ajustes de configuración avanzados. Esta extensión la usan también los escritorios GNOME (gswitchit) y KDE (kxkb).

SUGERENCIA: Información adicional

Puede obtener información adicional sobre XKB en el archivo `/etc/X11/xkb/README` y en los documentos ahí mencionados.

Puede encontrar información sobre la entrada de los idiomas chino, japonés y coreano (CJK) en la página de Mike Fabian: `http://www.suse.de/~mfabian/suse-cjk/input.html`.

10.4 Ajustes de idioma y país

Gracias a su gran nivel de internacionalización, SUSE Linux es muy flexible para adaptarse a las necesidades locales. En otras palabras, la internacionalización (*I18N*) permite implementar localizaciones (*L10N*) específicas. Las abreviaturas I18N y L10N hacen referencia a los términos ingleses "internationalization" y "localization" respectivamente: mencionan la letra inicial y final de cada palabra y el número de caracteres que se han omitido en medio.

Los ajustes se realizan mediante las variables `LC_` que se definen en el archivo `/etc/sysconfig/language`. No afectan sólo a la *compatibilidad con el idioma nativo,* sino también a las categorías de *mensajes* (idioma), *conjunto de caracteres, criterios de ordenación, fecha y hora, números* y *moneda.* Todas estas categorías se pueden definir directamente con su propia variable o de forma indirecta con una variable principal en el archivo `language` (consulte la página Man `locale`).

`RC_LC_MESSAGES`, `RC_LC_CTYPE`, `RC_LC_COLLATE`, `RC_LC_TIME`, `RC_LC_NUMERIC`, `RC_LC_MONETARY`
: Estas variables se pasan a la shell sin el prefijo `RC_` y representan las categorías indicadas arriba. A continuación, se describen los perfiles de shell en cuestión. El ajuste actual se puede mostrar con el comando `locale`.

`RC_LC_ALL`
: Esta variable, si se define, sobrescribe los valores de las variables mencionadas anteriormente.

`RC_LANG`
: Si no se define ninguna de las variables anteriores, ésta se usa como alternativa. Por defecto, SUSE Linux sólo define `RC_LANG`, lo que facilita el procedimiento a los usuarios a la hora de especificar sus propios valores.

`ROOT_USES_LANG`
: Se trata de una variable cuyos valores son `yes` (sí) y `no`. Si se define como `no`, el usuario `Root` funcionará siempre en el entorno POSIX.

Las variables se pueden definir mediante el editor sysconfig de YaST (consulte la Sección 8.3.1, “Cambio de la configuración del sistema mediante el editor YaST sysconfig” (p. 207)). El valor de una variable de este tipo incluye el código del idioma, el código del país, el tipo de codificación y el modificador. Todos estos componentes individuales se conectan mediante caracteres especiales:

```
LANG=<idioma>[[_<PAÍS>].<Codificación>[@<Modificador>]]
```

10.4.1 Ejemplos

Los códigos de idioma y país se deben definir juntos. El idioma sigue la norma ISO 639, que está disponible en http://www.evertype.com/standards/iso639/iso639-en.html y en http://www.loc.gov/standards/iso639-2/. Los códigos de países están definidos en la norma ISO 3166, que está disponible en http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html.

Sólo se pueden definir valores para los que haya archivos de descripción en /usr/lib/locale que se puedan utilizar. Se pueden crear archivos de descripción adicionales a partir de los archivos de /usr/share/i18n usando el comando localedef. Los archivos de descripción forman parte del paquete glibc-i18ndata. Se puede crear un archivo de descripción para es_ES.UTF-8 (para el español de España) con:

```
localedef -i es_ES@euro -f UTF-8 es_ES@euro.UTF-8
```

LANG=es_ES.UTF-8
: Éste es el ajuste por defecto si se selecciona el español de España durante la instalación. Si selecciona otro idioma, se habilitará dicho idioma, pero UTF-8 seguirá siendo el tipo de codificación de caracteres.

LANG=es_ES.ISO-8859-1
: De este modo se configura el idioma español para España con el juego de caracteres ISO-8859-1. Este juego de caracteres no admite el símbolo del euro, pero puede ser útil para los programas que no se hayan actualizado todavía para usar UTF-8. La cadena que define el conjunto de caracteres (ISO-8859-1, en este caso) la utilizan programas como Emacs.

LANG=es_ES@euro
: Este ejemplo incluye explícitamente el símbolo del euro en los ajustes del idioma. En realidad, este ajuste está obsoleto porque UTF-8 incluye también el símbolo del euro. Es útil sólo para las aplicaciones que no admitan UTF-8, sino ISO-8859-15.

SuSEconfig lee las variables de /etc/sysconfig/language y escribe los cambios necesarios en /etc/SuSEconfig/profile y en /etc/SuSEconfig/csh.cshrc. /etc/profile lee el archivo /etc/SuSEconfig/profile (lo usa

como *fuente*), mientras que `/etc/csh.cshrc` usa como fuente `/etc/SuSEconfig/csh.cshrc`. De esta forma, los ajustes están disponibles para todo el sistema.

Los usuarios pueden modificar los valores por defecto del sistema editando convenientemente el archivo `~/.bashrc`. Por ejemplo, si la configuración del sistema es español de España (`es_ES`) pero el usuario no desea que los mensajes de los programas se muestren en este idioma, deberá incluir, por ejemplo, `LC_MESSAGES=en_US` para que los mensajes se muestren en inglés de Estados Unidos.

10.4.2 Configuración regional en `~/.i18n`

Si no le satisfacen los valores por defecto de la configuración regional del sistema, puede cambiarlos en `~/.i18n`. Las entradas de `~/.i18n` sustituyen a los valores por defecto de `/etc/sysconfig/language`. Utilice los mismos nombres de variables sin los prefijos `RC_` del espacio de nombres. Por ejemplo, emplee `LANG` en lugar de `RC_LANG`.

10.4.3 Ajustes para la compatibilidad con el idioma

Los archivos de la categoría de *mensajes* normalmente se almacenan sólo en el directorio de idioma correspondiente (por ejemplo, `en`) para tener una alternativa. Si establece `LANG` en `en_US` y el archivo de mensajes de `/usr/share/locale/en_US/LC_MESSAGES` no existe, se usará como alternativa `/usr/share/locale/en/LC_MESSAGES`.

También se puede definir una cadena alternativa por ejemplo, para el bretón (en el caso del francés) o para el gallego (en el caso del español y el portugués):

```
LANGUAGE="br_FR:fr_FR"
```

```
LANGUAGE="gl_ES:es_ES:pt_PT"
```

Si lo desea, también puede usar las variantes noruegas nynorsk y bokmål (usando `no` como alternativa):

```
LANG="nn_NO"
```

```
LANGUAGE="nn_NO:nb_NO:no"
```

O bien

```
LANG="nb_NO"

LANGUAGE="nn_NO:nb_NO:no"
```

En el caso del noruego, hay que tener en cuenta que `LC_TIME` también se trata de forma diferente.

Un problema que puede surgir es que el separador utilizado para delimitar grupos de dígitos no se reconozca correctamente. Esto ocurre si `LANG` está establecido sólo como un código de idioma de dos letras como, por ejemplo, `de`, y la definición que utiliza glibc se encuentra en `/usr/share/lib/de_DE/LC_NUMERIC`. En este caso, `LC_NUMERIC` debe configurarse como `de_DE` para que la definición del separador sea evidente para el sistema.

10.4.4 Información adicional

- *El GNU C Library Reference Manual* (Manual de referencia sobre la biblioteca C de GNU), capítulo “Locales and Internationalization” (Configuraciones regionales e internacionalización). Se incluye en `glibc-info`.
- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux* (Preguntas frecuentes sobre Unicode y UTF-8 para Unix y Linux), en `http://www.cl.cam.ac.uk/~mgk25/unicode.html`.
- Bruno Haible, *Unicode-Howto* (Procedimientos de Unicode): `/usr/share/doc/howto/en/html/Unicode-HOWTO.html`.

11 Funcionamiento de la impresora

CUPS es el sistema de impresión estándar de SUSE Linux. CUPS está muy orientado al usuario. En muchos casos, es compatible con LPRng o puede adaptarse de forma relativamente fácil. LPRng se incluye en SUSE Linux únicamente por razones de compatibilidad.

Las impresoras pueden distinguirse por la interfaz, como de puerto USB o de red, y por el lenguaje de impresión. Al comprar una impresora, asegúrese de que tiene una interfaz compatible con el hardware y un lenguaje de impresión adecuado. Las impresoras se pueden clasificar en función de los tres lenguajes de impresión siguientes:

Impresoras PostScript
: PostScript es el lenguaje de impresión en el que la mayor parte de los trabajos de impresión de Linux y Unix se generan y se procesan por el sistema de impresión interno. Es un lenguaje ya bastante antiguo y, aun así, muy eficaz. Si la impresora puede procesar directamente documentos PostScript y no es necesaria una conversión posterior de éstos en el sistema de impresión, se reduce el número de fuentes de errores posibles. Puesto que las impresoras PostScript están sujetas a cuantiosos costes de licencia, normalmente su precio es superior al del resto de impresoras que no disponen de un intérprete PostScript.

Impresora estándar (lenguajes como PCL y ESC/P)
: Aunque estos lenguajes de impresión son bastante antiguos, continúa su expansión para hacer frente a las nuevas funciones de las impresoras. En el caso de lenguajes de impresión conocidos, el sistema de impresión puede convertir trabajos PostScript al lenguaje correspondiente con la ayuda de Ghostscript. Esta fase del proceso se denomina "interpretación". Los lenguajes más conocidos son PCL, que se utiliza sobre todo con impresoras HP y sus clónicas, y ESC/P, que utilizan las impresoras

Epson. Estos lenguajes de impresión son, por lo general, compatibles con Linux y tienen como resultado una impresión de notable calidad. Es posible que Linux no admita algunas funciones de impresoras extremadamente nuevas y sofisticadas, ya que los desarrolladores de código abierto pueden estar trabajando aún en ellas. A excepción de los controladores `hpijs` desarrollados por HP, actualmente no hay ningún fabricante de impresoras que desarrolle controladores Linux y los ponga a disposición de los distribuidores de Linux con licencia de código abierto. La mayor parte de estas impresoras tienen un precio medio.

Impresoras con lenguaje de impresión propio (normalmente impresoras GDI)
: Normalmente, tan sólo hay uno o varios controladores de Windows disponibles para las impresoras con lenguaje de impresión propio. Son impresoras que no admiten ninguno de los lenguajes de impresión habituales y que utilizan un lenguaje sujeto a cambio al iniciarse una nueva versión del modelo en cuestión. Si desea obtener más información, consulte la Sección 11.7.1, “Impresoras sin compatibilidad con lenguaje de impresión estándar” (p. 264).

Antes de comprar una nueva impresora, compruebe su compatibilidad en las siguientes fuentes:

- `http://cdb.suse.de/` (base de datos de impresoras de SUSE Linux)
- `http://www.linuxprinting.org/` (base de datos de impresoras de LinuxPrinting.org)
- `http://www.cs.wisc.edu/~ghost/` (página web de Ghostscript)
- `/usr/share/doc/packages/ghostscript/catalog.devices` (lista de controladores incluidos)

Las bases de datos en línea siempre especifican el estado de compatibilidad con Linux más actualizado. No obstante, una distribución Linux tan sólo puede integrar los controladores disponibles en el momento de producción. Por lo tanto, es posible que una impresora que tenga, en un momento dado, el estado “perfectly supported” (compatibilidad perfecta) no tuviera este estado cuando se inició la última versión de SUSE Linux. De este modo, las bases de datos no indican necesariamente el estado correcto, sino que sólo proporcionan una aproximación.

11.1 Flujo de trabajo del sistema de impresión

El usuario crea un trabajo de impresión. Este trabajo consta de datos que van a imprimirse, junto con información para el gestor de cola, como el nombre de la impresora o el nombre de la cola de impresión y, de forma opcional, información para el filtro, como las opciones de la impresora específica.

Hay una cola de impresión específica para cada impresora. El gestor de cola puede mantener el trabajo de impresión en la cola hasta que la impresora deseada se encuentre preparada para la recepción de datos. Cuando esté lista, el gestor de cola enviará a la impresora los datos mediante el filtro y el sistema secundario.

El filtro convierte los datos que el usuario desea imprimir (ASCII, PostScript, PDF, JPEG, etc.) a los datos de la impresora específica (PostScript, PCL, ESC/P, etc.). Las funciones de la impresora se describen en los archivos PPD. Un archivo PPD contiene las opciones de impresora específica con los parámetros necesarios para habilitarlas en la impresora. El sistema de filtros comprueba que las opciones seleccionadas por el usuario estén habilitadas.

Si utiliza una impresora PostScript, el sistema de filtros convierte los datos a PostScript de la impresora específica. Para ello, no se necesita un controlador de impresora. Si utiliza una impresora que no sea PostScript, el sistema de filtros convierte los datos a los de la impresora específica mediante Ghostscript. Para ello, se necesita un controlador de impresora Ghostscript adecuado para su impresora. El sistema secundario recibe del filtro los datos de la impresora específica y los transfiere a la impresora.

11.2 Métodos y protocolos de conexión de impresoras

Hay varias posibilidades de conexión de una impresora al sistema. La configuración del sistema de impresión CUPS no distingue entre una impresora local y una impresora conectada al sistema a través de la red. Las impresoras locales, en Linux, deben conectarse de la forma descrita en el manual del fabricante de la impresora. CUPS admite conexiones en serie, USB, paralelas y SCSI. Para obtener más información sobre la conexión de impresoras, consulte el artículo *CUPS in a Nutshell* (CUPS en pocas

palabras) en la base de datos de asistencia en http://portal.suse.com. Para encontrar el artículo, escriba *cups* en el cuadro de diálogo de búsqueda.

AVISO: Conexión por cable a la máquina

Al conectar la impresora a la máquina, recuerde que tan sólo los dispositivos USB pueden conectarse y desconectarse durante el funcionamiento. El sistema debería cerrarse antes de cambiar otro tipo de conexiones.

11.3 Instalación del software

PPD (Descripción de impresora PostScript) es el lenguaje que describe las propiedades, como la resolución, y las opciones, como la disponibilidad de unidad dúplex. Estas descripciones son necesarias para utilizar varias opciones de impresora en CUPS. Sin un archivo PPD, los datos de impresión serán reenviados a la impresora "en bruto", lo que no resulta conveniente. A lo largo de la instalación de SUSE Linux, muchos archivos PPD se preinstalan para que puedan usarse incluso en impresoras que no admitan PostScript.

Para configurar una impresora PostScript, el mejor método es conseguir un archivo PPD. Hay muchos archivos PPD disponibles en el paquete `manufacturer-PPDs`, que se instala automáticamente aun con una instalación estándar. Consulte la Sección 11.6.3, "Archivos PPD en varios paquetes" (p. 261) y la Sección 11.7.2, "Inexistencia de archivo PPD adecuado para una impresora PostScript" (p. 265).

Los archivos PPD nuevos pueden almacenarse en el directorio `/usr/share/cups/model/` o añadirse al sistema de impresión con YaST (consulte "Configuración manual" (p. 252)). Posteriormente, el archivo PPD podrá seleccionarse durante la instalación.

Tenga cuidado en el caso de que un fabricante de impresoras le indique que instale paquetes de software completos y que, además, modifique los archivos de configuración. En primer lugar, este tipo de instalación tendría como resultado la pérdida de la compatibilidad que SUSE Linux proporciona; y, en segundo lugar, es posible que los comandos de impresión funcionaran de forma distinta y que dispositivos de otros fabricantes dejaran de funcionar en el sistema. Por esta razón, no se recomienda efectuar la instalación del software del fabricante.

11.4 Configuración de la impresora

Tras conectar la impresora al equipo e instalar el software, instale la impresora en el sistema. Esta instalación debería llevarse a cabo utilizando las herramientas que se distribuyen con SUSE Linux. Dado que SUSE Linux hace especial hincapié en la seguridad, las herramientas de otros fabricantes a menudo presentan ciertas dificultades con respecto a las restricciones de seguridad y, con ello, dan lugar a más problemas que ventajas. Consulte la Sección 11.6.1, “Servidor y cortafuegos CUPS” (p. 258) y la Sección 11.6.2, “Cambios en el servicio de impresión CUPS” (p. 259) para obtener más información sobre la solución de problemas.

11.4.1 Impresoras locales

Si se detecta una impresora local sin configurar al iniciar sesión, YaST comienza a configurarla. Para ello, se utilizan los mismos cuadros de diálogo que en la descripción de la configuración siguiente.

Para configurar la impresora, seleccione *Hardware* → *Printer* (Hardware - Impresora) en el centro de control de YaST. Con esto, se abre la ventana principal de configuración de la impresora, en cuya parte superior se enumeran los dispositivos detectados. En la parte inferior se enumeran todas las colas configuradas hasta ese momento. Si no se ha detectado la impresora, configúrela manualmente.

IMPORTANTE

Si la entrada *Printer* (Impresora) no se encuentra disponible en el centro de control de YaST, es probable que el paquete `yast2-printer` no esté instalado. Para solucionar este problema, instale el paquete `yast2-printer` y reinicie YaST.

Configuración automática

YaST podrá configurar la impresora de forma automática si el puerto paralelo o USB puede configurarse automáticamente y se puede detectar la impresora conectada. La base de datos de la impresora también debe contener la cadena de ID de la impresora que YaST recupera durante la detección automática de hardware. Si el ID del hardware no coincide con la designación del modelo, seleccione este último manualmente.

Para asegurarse de que todo funciona correctamente, todo valor de configuración debe comprobarse con la función de prueba de impresión de YaST. La página de prueba también proporciona información relevante sobre la configuración sobre la que se ha efectuado la prueba.

Configuración manual

Si no se cumplen los requisitos de la configuración automática o si desea una personalizada, configure la impresora manualmente. Es posible que YaST sea capaz de determinar automáticamente los ajustes correctos o, al menos, hacer una selección previa razonable en función de la corrección de la detección automática y la cantidad de información sobre el modelo de impresora que se encuentre en la base de datos.

Deben configurarse los siguientes parámetros:

Hardware Connection (Port) (Conexión de hardware [Puerto])
: La configuración de la conexión de hardware depende de que YaST haya sido capaz de hallar la impresora durante la detección automática del hardware. Si YaST ha sido capaz de detectar el modelo de impresora automáticamente, se puede suponer que la conexión de la impresora funciona en el nivel de hardware y los ajustes no necesitan cambios al respecto. Si YaST no es capaz de detectar el modelo de la impresora, puede haber algún problema con la conexión en el nivel de hardware. En tal caso, la configuración de la conexión exige cierta intervención manual.

  En el cuadro de diálogo *Configuración de la impresora,* haga clic en *Añadir* para iniciar el flujo de trabajo de configuración manual. En el mismo cuadro, seleccione el valor *Printer Type* (Tipo de impresora) que le corresponda (por ejemplo `USB printer` [Impresora USB]) y, mediante *Next* (Siguiente), especifique el valor de *Printer Connection* (Conexión de la impresora) y seleccione el dispositivo.

Name of the Queue (Denominación de la cola)
: El nombre de la cola se utiliza con los comandos de impresión. Este nombre debería ser relativamente corto y estar formado exclusivamente por letras minúsculas y números. En el cuadro de diálogo siguiente (*Queue name* [Nombre de la cola]), especifique el valor de *Name for printing* (Nombre para la impresión).

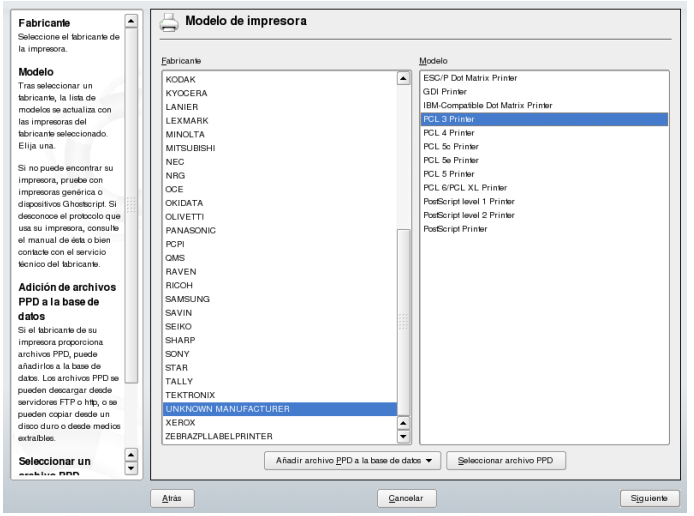
Modelo de la impresora y archivo PPD
: Todos los parámetros de la impresora específica, como el controlador Ghostscript que se va a utilizar y los parámetros del filtro de la impresora, se almacenan en un

archivo PPD (Descripción de impresora PostScript). Para obtener más información sobre los archivos PPD, consulte la Sección 11.3, “Instalación del software” (p. 250).

Para muchos modelos de impresora, están disponibles varios archivos PPD (por ejemplo, en el caso de que varios controladores Ghostscript funcionen en el modelo en cuestión). Al seleccionar un fabricante y un modelo en el cuadro de diálogo siguiente (*Printer model* [Modelo de impresora]), seleccione el archivo PPD que le corresponde a la impresora. Si varios archivos PPD se encuentran disponibles para ese modelo, YaST establece uno de ellos por defecto (normalmente, el que aparece marcado como `recommended` [recomendado]). Puede cambiar el archivo PPD seleccionado en el siguiente cuadro de diálogo con *Edit* (Editar).

Para los modelos que no sean PostScript, el controlador Ghostscript crea todos los datos de la impresora específica. Por esta razón, la configuración del controlador es el factor individual de mayor importancia en la determinación de la calidad de impresión. El tipo de controlador Ghostscript (archivo PPD) seleccionado y las opciones que para él se especifican determinan la calidad de impresión. En caso necesario, cambie las opciones adicionales (que el archivo PPD pone a su disposición) tras seleccionar*Edit* (Editar).

Figura 11.1 *Selección del modelo de la impresora*



Imprima siempre la página de prueba para comprobar que los ajustes funcionan como es debido. Si el resultado no es el esperado (con varias páginas casi vacías,

por ejemplo), debería poder interrumpir el funcionamiento de la impresora retirando todo el papel y, a continuación, deteniendo la prueba desde YaST.

Si la base de datos de la impresora no incluye ninguna entrada para su modelo, puede añadir un archivo PPD nuevo (seleccionando *Add PPD File to Database* [Añadir archivo PPD a la base de datos]) o utilizar un conjunto de archivos PPD genéricos para hacer que la impresora funcione con uno de los lenguajes de impresión estándar. Para ello, seleccione *UNKNOWN MANUFACTURER* (Fabricante desconocido) como su fabricante de impresora.

Advanced Settings (Ajustes avanzados)
: Por lo general, no necesita efectuar ningún cambio en estos ajustes.

11.4.2 Impresoras de red

Una impresora de red admite varios protocolos, algunos de ellos incluso de forma simultánea. Aunque la mayor parte de los protocolos admitidos son estandarizados, algunos fabricantes pueden expandir (modificar) el estándar porque llevan a cabo pruebas en sistemas que aún no lo aplican correctamente o porque quieren proporcionar ciertas funciones que no están disponibles con el estándar en cuestión. Los fabricantes proporcionan controladores únicamente para unos pocos sistemas operativos, con lo que eliminan las dificultades que surgen con esos sistemas. Desafortunadamente, en contadas ocasiones se proporcionan controladores para Linux. La situación actual impide dar por sentado que todo protocolo funciona sin problemas en Linux. Por lo tanto, es posible que necesite probar con varias opciones para lograr una configuración funcional.

CUPS admite los protocolos `LPD`, `IPP` y `SMB` y de `socket`. A continuación se presenta información detallada sobre estos protocolos:

Socket (zócalo)
: *Socket* (zócalo) hace referencia a una conexión que permite el envío de datos a un zócalo de Internet sin efectuar antes un acuerdo de datos. Algunos de los números de puerto de zócalos usados con mayor frecuencia son `9100` o `35`. Un ejemplo de URI de dispositivo es `socket://host-printer:9100/`.

LPD (daemon de impresora de línea)
: El protocolo LPD probado se describe en RFC 1179. Bajo este protocolo, algunos datos relacionados con trabajos, como el ID de la cola de impresión, se envían antes que los propios datos de impresión. Por lo tanto, debe especificarse una cola de

impresión al configurar el protocolo LPD para la transmisión de datos. Los productos de varios fabricantes de impresoras son lo suficientemente flexibles como para aceptar cualquier nombre para la cola de impresión. Si fuera necesario, el manual de la impresora debería indicar qué nombre utilizar. A menudo se utilizan nombres como LPT, LPT1, LP1 o similares. También puede configurarse una cola LPD en un host Linux o Unix diferente en el sistema CUPS. El número de puerto de un servicio LPD es `515`. Un ejemplo de URI de dispositivo es `lpd://host-printer/LPT1`.

IPP (Protocolo de impresión de Internet)
: IPP es un protocolo relativamente nuevo (1999) basado en el protocolo HTTP. Con IPP, se transmite una cantidad mayor de datos relacionados con el trabajo que con otros protocolos. CUPS utiliza IPP para la transmisión de datos internos. Este es el protocolo más utilizado para el reenvío de colas entre dos servidores CUPS. El nombre de la cola de impresión es necesario para la configuración correcta de IPP. El número de puerto para SIP es el `631.` Dos ejemplos de URI de dispositivo son `ipp://host-printer/ps` y `ipp://host-cupsserver/printers/ps`.

SMB (Recurso compartido de Windows)
: CUPS también admite la impresión en impresoras conectadas a recursos compartidos de Windows. El protocolo que se utiliza para tal propósito es SMB. SMB utiliza los números de puerto `137`, `138` y `139`. `smb://user:password@workgroup/server/printer`, `smb://user:password@host/printer` y `smb://server/printer` son varios ejemplos de URI de dispositivo.

El protocolo que admite la impresora debe determinarse antes de la configuración. Si el fabricante no proporciona la información necesaria, el comando `nmap`, que viene con el paquete `nmap`, puede utilizarse para averiguar el protocolo. `nmap` comprueba todos los puertos abiertos de un host. Por ejemplo:

```
nmap -p 35,137-139,515,631,9100-10000 printerIP
```

Configuración de CUPS en una red mediante YaST

Las impresoras de red deben configurarse mediante YaST. YaST facilita el procedimiento de configuración y está óptimamente equipado para vencer las restricciones de seguridad de CUPS (consulte la Sección 11.6.2, “Cambios en el servicio de impresión CUPS” (p. 259)). Para informarse sobre las directrices de instalación de CUPS en una

red, consulte el artículo *CUPS in a Nutshell* (CUPS en pocas palabras) en la base de datos de asistencia en `http://portal.suse.com`.

Inicie la configuración de la impresora y haga clic en *Añadir*. Salvo que el administrador de red especifique lo contrario, pruebe con la opción *Print Directly to a Network Printer* (Imprimir directamente en impresora de red) y siga el procedimiento local correspondiente.

Configuración mediante herramientas de líneas de comando

De forma alternativa, CUPS puede configurarse con herramientas de línea de comando como `lpadmin` y `lpoptions`. Se necesita un URI (Identificador de recurso uniforme) que conste de un sistema secundario, como usb, además de parámetros como `/dev/usb/lp0`. Por ejemplo, el URI completo podría ser `parallel:/dev/lp0` (impresora conectada al primer puerto paralelo) o `usb:/dev/usb/lp0` (primera impresora detectada, conectada al puerto USB).

Con `lpadmin`, el administrador de servidor CUPS puede añadir, eliminar o gestionar colas de clase y de impresión. Para añadir una cola de impresión, utilice la siguiente sintaxis:

```
lpadmin -p queue -v device-URI \
-P PPD-file -E
```

Con ello, el dispositivo (`-v`) se encontrará disponible como *`queue`* (`-p`) mediante el archivo PPD especificado (`-P`). Esto significa que debe saber cuál es el archivo PPD y el nombre del dispositivo si desea configurar la impresora manualmente.

No utilice `-E` como primera opción. Para todos los comandos CUPS, si `-E` se utiliza como primer argumento, se establece una conexión cifrada. Para habilitar la impresora, debe utilizarse `-E` como se muestra en el siguiente ejemplo:

```
lpadmin -p ps -v parallel:/dev/lp0 -P \
/usr/share/cups/model/Postscript.ppd.gz -E
```

El siguiente ejemplo ilustra la cómo configurar una impresora de red:

```
lpadmin -p ps -v socket://192.168.1.0:9100/ -P \
/usr/share/cups/model/Postscript-level1.ppd.gz -E
```

Para conocer más opciones de `lpadmin`, consulte la página Man de `lpadmin(1)`.

Durante la configuración de la impresora, algunas opciones se establecen como valor por defecto. Estas opciones pueden modificarse en cada trabajo de impresión (en función del uso de la herramienta de impresión). También es posible cambiar con YaST estas opciones por defecto. Mediante herramientas de línea de comando, establezca las opciones como por defecto como se especifica a continuación:

1. En primer lugar, enumere todas las opciones:

   ```
   lpoptions -p queue -l
   ```

   Ejemplo:

   ```
   Resolution/Output Resolution: 150dpi *300dpi 600dpi
   ```

   La opción por defecto activada se marca anteponiendo un asterisco (`*`).

2. Cambie la opción con `lpadmin`:

   ```
   lpadmin -p queue -o Resolution=600dpi
   ```

3. Compruebe el nuevo ajuste:

   ```
   lpoptions -p queue -l

   Resolution/Output Resolution: 150dpi 300dpi *600dpi
   ```

Cuando un usuario normal ejecuta `lpoptions`, los ajustes se escriben en `~/.lpoptions`. Los ajustes del usuario `Root` se escriben en `/etc/cups/lpoptions`.

11.5 Configuración para aplicaciones

Las aplicaciones utilizan las colas de impresión existentes del mismo modo en que lo hacen las herramientas de línea de comandos. Normalmente, no es necesario volver a configurar la impresora para una aplicación concreta, puesto que debería ser capaz de imprimir desde aplicaciones utilizando las colas disponibles.

Para imprimir desde la línea de comandos, escriba `lp -d` *`nombredecola nombredearchivo`*, sustituyendo *`nombredecola`* y *`nombredearchivo`* por los nombres correspondientes.

Algunas aplicaciones utilizan el comando `lp` para llevar a cabo la impresión. En estos casos, escriba el comando correcto en el cuadro de diálogo de impresión de la aplicación (normalmente sin especificar *`nombredearchivo`*); por ejemplo, `lp -d` *`nombredecola`*. Para hacer esto con programas de KDE, habilite *Print through an external program* (Imprimir mediante programa externo). En caso contrario, no podrá introducir el comando de impresión.

Herramientas como xpp y kprinter del programa de KDE proporcionan una interfaz gráfica para elegir entre colas y definir las opciones estándar de CUPS y las opciones de la impresora específica que se habilitan gracias al archivo PPD. Puede utilizar kprinter como la interfaz de impresión estándar de las aplicaciones que no sean de KDE, especificando `kprinter` o `kprinter --stdin` como el comando de impresión en los cuadros de diálogo de las aplicaciones en cuestión. El comportamiento mismo de la aplicación determina cuál de estos dos comandos utilizar. Si se configura correctamente, la aplicación debería llamar al cuadro de diálogo de kprinter siempre que la primera dé lugar a un trabajo de impresión. De este modo, puede utilizar el cuadro de diálogo para seleccionar una cola y definir otras opciones de impresión. Esto requiere que la propia configuración de impresión de la aplicación no entre en conflicto con la de kprinter y que las opciones de impresión tan sólo se cambien mediante kprinter después de su habilitación.

11.6 Funciones especiales en SUSE Linux

Se ha llevado a cabo una adaptación de varias funciones de CUPS para SUSE Linux. Aquí se tratan algunos de los cambios más importantes.

11.6.1 Servidor y cortafuegos CUPS

Hay varias formas de configurar CUPS como cliente de un servidor de red.

1. Para cada cola del servidor de red, puede configurar una cola local para reenviar todos los trabajos al servidor de red correspondiente (cola de reenvío). Por lo general, no se recomienda hacer esto, puesto que todas las máquinas clientes deben configurarse nuevamente siempre que cambie la configuración del servidor de red.

2. Los trabajos de impresión también pueden reenviarse directamente a un servidor de red. Para este tipo de configuración, no ejecute un daemon CUPS local. `lp` o las llamadas a las bibliotecas correspondientes a otros programas pueden enviar trabajos directamente al servidor de red. No obstante, esta configuración no funciona si también desea imprimir en una impresora local.

3. El daemon CUPS puede escuchar a los paquetes de difusión IPP que envían otros servidores de red para anunciar las colas disponibles.

   Esta es la mejor configuración CUPS para imprimir en servidores CUPS remotos. No obstante, existe el riesgo de que un atacante envíe difusiones IPP con colas y de que el daemon local acceda a la cola falsa. Si entonces se muestra la cola con el mismo nombre que el de otra cola del servidor local, es posible que el propietario del trabajo crea que éste se ha enviado a un servidor local, cuando en realidad se ha enviado al servidor del atacante.

YaST puede detectar servidores CUPS explorando todos los hosts de la red local para comprobar si ofrecen el servicio IPP o escuchando las difusiones IPP. Para ello es preciso que el cortafuegos permita los paquetes entrantes en el puerto 631/UDP (cliente del servicio IPP), lo que se habilita automáticamente cuando se configura el equipo para que resida en la zona interna del cortafuegos. Si se abre un puerto para configurar el acceso a colas remotas en la zona externa, puede suponer un riesgo para la seguridad, porque los posibles atacantes podrían difundir un servidor que fuese aceptado por los usuarios. Por defecto, las difusiones IPP se rechazan en la zona externa. Consulte "Configuración con YaST" (p. 116) para obtener información detallada acerca de la configuración del cortafuegos.

De forma alternativa, los usuarios pueden detectar servidores CUPS explorando activamente los hosts de red local o configurar todas las colas manualmente. No obstante, este método no se recomienda a causa de las razones que se mencionaron al comienzo de esta sección.

11.6.2 Cambios en el servicio de impresión CUPS

Estos cambios se aplicaron inicialmente para SUSE Linux 9.1.

Ejecución de cupsd el usuario lp

Al iniciarse, `cupsd` cambia del usuario `root` al usuario `lp`. Con ello, se proporciona un nivel de seguridad muy superior, ya que el servicio de impresión CUPS no se ejecuta con permisos sin restricciones, sino únicamente con los permisos necesarios para el servicio de impresión.

No obstante, la autenticación (comprobación de la contraseña) no puede efectuarse mediante `/etc/shadow`, puesto que `lp` no tiene acceso a `/etc/shadow`. En lugar de esto, debe utilizarse la autenticación del CUPS específico por medio de `/etc/cups/passwd.md5`. Para ello, deben especificarse en `/etc/cups/passwd.md5` un administrador CUPS con el grupo de administración CUPS `sys` y una contraseña CUPS. Esto se consigue escribiendo lo que aparece a continuación como `root`:

```
lppasswd -g sys -a CUPS-admin-name
```

Este ajuste resulta esencial también si se desea utilizar la interfaz Web de administración de CUPS o la herramienta de administración de impresoras de KDE.

Cuando `cupsd` se ejecuta como `lp`, `/etc/printcap` no puede generarse, puesto que no se le permite a `lp` crear archivos en `/etc/`. Por lo tanto, `cupsd` crea `/etc/cups/printcap`. Para garantizar que las aplicaciones que sólo pueden leer nombres de cola de `/etc/printcap` sigan funcionando correctamente, `/etc/printcap` actúa como un enlace simbólico que apunta a `/etc/cups/printcap`.

Cuando `cupsd` se ejecuta como `lp`, el puerto `631` no puede abrirse. Por lo tanto, `cupsd` no puede recargarse con `rccups reload`. En lugar de este comando, utilice `rccups restart`.

Funciones generalizadas para `BrowseAllow` y `BrowseDeny`

Los permisos de acceso definidos para `BrowseAllow` y `BrowseDeny` se aplican a todos los tipos de paquetes enviados a `cupsd`. Los ajustes por defecto en `/etc/cups/cupsd.conf` son los siguientes:

```
BrowseAllow @LOCAL
BrowseDeny All
```

y

```
<Location />
  Order Deny,Allow
  Deny From All
  Allow From 127.0.0.1
  Allow From 127.0.0.2
  Allow From @LOCAL
</Location>
```

De este modo, tan sólo los hosts `LOCAL` pueden tener acceso a `cupsd` en un servidor CUPS. Los hosts `LOCAL` son hosts cuyas direcciones IP pertenecen a una interfaz que no es PPP (interfaces cuyos indicadores `IFF_POINTOPOINT` no se han establecido) y a la misma red que el servidor CUPS. Los paquetes de todos los otros hosts se rechazan inmediatamente.

Activación por defecto de cupsd

En una instalación estándar, `cupsd` se activa automáticamente, con lo que se habilita un acceso cómodo a las colas de los servidores de red CUPS sin ninguna acción manual adicional. Los elementos que aparecen en "Ejecución de cupsd el usuario lp" (p. 260) y "Funciones generalizadas para `BrowseAllow` y `BrowseDeny`" (p. 260) son condiciones previas fundamentales para esta función, puesto que, de lo contrario, la seguridad no sería suficiente como para efectuar una activación automática de `cupsd`.

11.6.3 Archivos PPD en varios paquetes

La configuración de impresora YaST configura las colas para CUPS utilizando únicamente los archivos PPD instalados en `/usr/share/cups/model/` en el sistema. Para encontrar los archivos PPD adecuados para el modelo de la impresora, YaST compara el proveedor y el modelo determinados a lo largo de la detección del hardware con aquellos que figuran en todos los archivos PPD disponibles en `/usr/share/cups/model/` en el sistema. Para ello, la configuración de impresora YaST genera una base de datos a partir de la información del proveedor y del modelo extraída de los archivos PPD. Al seleccionar una impresora de la lista de proveedores y modelos, recibirá los archivos PPD que coincidan con el proveedor y el modelo.

La configuración que utiliza únicamente archivos PPD y ninguna otra fuente de información distinta presenta la ventaja de que los archivos PPD en `/usr/share/cups/model/` pueden modificarse sin restricción alguna. La configuración de impresora YaST reconoce los cambios y regenera la base de datos de proveedores y modelos. Por ejemplo, si tan sólo se dispone de impresoras PostScript, por lo general no se necesitarán

los archivos PPD Foomatic del paquete `cups-drivers` o los archivos PPD Gimp-Print del paquete `cups-drivers-stp`. En lugar de esto, los archivos PPD para las impresoras PostScript pueden copiarse directamente en `/usr/share/cups/model/` (si no existen ya en el paquete `manufacturer-PPDs`) para lograr una configuración óptima de las impresoras.

Archivos PPD CUPS del paquete `cups`

A los archivos PPD genéricos del paquete `cups` se les ha añadido, como complemento, archivos PPD Foomatic adaptados para impresoras PostScript de nivel 1 y nivel 2:

- `/usr/share/cups/model/Postscript-level1.ppd.gz`
- `/usr/share/cups/model/Postscript-level2.ppd.gz`

Archivos PPD del paquete `cups-drivers`

Por lo general, el filtro de impresora Foomatic `foomatic-rip` se utiliza junto con Ghostscript para impresoras que no son PostScript. Los archivos PPD Foomatic adecuados tienen las entradas `*NickName: ... Foomatic/Ghostscript driver` y `*cupsFilter: ... foomatic-rip`. Estos archivos PPD se encuentran en el paquete `cups-drivers`.

YaST prefiere un archivo PPD Foomatic si un archivo PPD Foomatic con la entrada `*NickName: ... Foomatic ... (recommended)` coincide con el modelo de impresora y el paquete `manufacturer-PPDs` no contiene un archivo PPD más adecuado.

Archivos PPD Gimp-Print del paquete `cups-drivers-stp`

En lugar de `foomatic-rip`, el filtro CUPS `rastertoprinter` de Gimp-Print puede utilizarse para varias impresoras que no sean PostScript. Este filtro y los archivos PPD de Gimp-Print adecuados están disponibles en el paquete `cups-drivers-stp`. Los archivos PPD de Gimp-Print se encuentran en `/usr/share/cups/model/stp/` y tienen las entradas `*NickName: ... CUPS+Gimp-Print` y `*cupsFilter: ... rastertoprinter`.

Archivos PPD de fabricantes de impresoras del paquete `manufacturer-PPDs`

El paquete `manufacturer-PPDs` contiene archivos PPD de fabricantes de impresoras que se comercializan con una licencia de carácter suficientemente liberal. Las impresoras PostScript deberían configurarse con el archivo PPD adecuado del fabricante de impresoras, puesto que este archivo permite utilizar todas las funciones de la impresora PostScript. YaST prefiere un archivo PPD del paquete `manufacturer-PPDs` siempre que se cumplan las siguientes condiciones:

- El proveedor y el modelo determinados a lo largo de la detección del hardware coincide con el proveedor y el modelo que figura en un archivo PPD del paquete `manufacturer-PPDs`.

- El archivo PPD del paquete `manufacturer-PPDs` es el único disponible para el modelo de impresora o hay un archivo PPD Foomatic con una entrada `*NickName: ... Foomatic/Postscript (recommended)` que también coincide con el modelo de impresora.

En consecuencia, YaST no utiliza ningún archivo PPD del paquete `manufacturer-PPDs` en los siguientes casos:

- El archivo PPD del paquete `manufacturer-PPDs` no coincide con el proveedor y el modelo. Esto puede ocurrir si el paquete `manufacturer-PPDs` contiene únicamente un archivo PPD para los modelos similares; por ejemplo, en el caso de que no haya ningún archivo PPD separado para los modelos particulares de una serie determinada, pero el nombre del modelo se especifique (como `Funprinter 1000 series`, por ejemplo) en el archivo PPD.

- No se recomienda el archivo PPD PostScript de Foomatic. Puede que la causa de esto radique en que el modelo de impresora no funciona con suficiente eficacia en el modo PostScript; por ejemplo, la impresora puede ser poco fiable en este modo por tener demasiado poca memoria, o ser demasiado lenta a causa de la excesiva debilidad de su procesador. Además, es posible que la impresora no admita PostScript por defecto; por ejemplo, puede ocurrir que la compatibilidad con PostScript tan sólo esté disponible gracias a un módulo opcional.

Si un archivo PPD del paquete `manufacturer-PPDs` es adecuado para una impresora PostScript, pero YaST no puede configurarla por las razones indicadas, seleccione manualmente en YaST el modelo respectivo de impresora.

11.7 Solución de problemas

Las secciones siguientes se ocupan de algunos de los problemas relacionados con el software y el hardware de la impresora que aparecen con más frecuencia y ofrece propuestas para solucionarlos o eludirlos.

11.7.1 Impresoras sin compatibilidad con lenguaje de impresión estándar

Las impresoras que no admiten ningún lenguaje de impresión habitual y con las que tan sólo es posible comunicarse mediante secuencias de control especiales se denominan *impresoras GDI*. Estas impresoras sólo pueden funcionar con las versiones del sistema operativo para las que exista un controlador comercializado por el fabricante. *GDI* es una interfaz de programación desarrollada por Microsoft para dispositivos de gráficos. El verdadero problema no radica en la interfaz de programación, sino en el hecho de que sólo es posible comunicarse con las impresoras GDI mediante el lenguaje de impresión propio del modelo de impresora específica.

En el caso de algunas impresoras, puede cambiarse del funcionamiento en modo GDI a uno de los lenguajes de impresión estándar. Algunos fabricantes proporcionan controladores propios para sus impresoras GDI. El inconveniente que presenta este tipo de controladores es que no se garantiza su funcionamiento con el sistema de impresión instalado, además de que no resultan adecuados para las distintas plataformas de hardware. Por contra, las impresoras que admiten un lenguaje de impresión estándar no dependen de una versión del sistema de impresión ni de una plataforma de hardware especiales.

En lugar de dedicar el tiempo a intentar hacer funcionar un controlador Linux para una marca concreta, podría resultar más rentable adquirir una impresora compatible. Esto resolvería el problema con el controlador de una vez por todas, con lo que se eliminaría la necesidad de instalar y configurar el software especial del controlador, junto con la de conseguir las actualizaciones de éste que podrían precisarse a raíz de desarrollos posteriores del sistema de impresión.

11.7.2 Inexistencia de archivo PPD adecuado para una impresora PostScript

Si el paquete `manufacturer-PPDs` no contiene ningún archivo PPD adecuado para una impresora PostScript, debería ser posible utilizar el archivo PPD desde el CD del controlador del fabricante de la impresora, o descargar un archivo PPD adecuado de la página Web del fabricante.

Si el archivo PPD se suministra en formato zip (.zip) o como archivo zip de extracción automática (`.exe`), descomprímalo mediante `unzip`. En primer lugar, revise las cláusulas de la licencia del archivo PPD. A continuación, utilice la utilidad `cupstestppd` para comprobar si el archivo PPD cumple la "Adobe PostScript Printer Description File Format Specification, version 4.3." (Versión 4.3 de la Especificación de formato de archivo de descripción de impresora PostScript de Adobe). Si la utilidad devuelve el valor "FAIL", hay errores serios en los archivos PPD y es probable que causen problemas importantes. Los problemas de los que informe `cupstestppd` deben eliminarse. En caso necesario, solicite un archivo PPD adecuado al fabricante de la impresora.

11.7.3 Puertos paralelos

El procedimiento más seguro consiste en conectar directamente la impresora al primer puerto paralelo y seleccionar los ajustes de puerto paralelo siguientes en el BIOS:

- I/O address: `378` (hexadecimal)
- Interrupt: irrelevante
- Mode: `Normal`, `SPP` o `Output Only`
- DMA: inhabilitado

Si, pese a estos ajustes, no es posible la comunicación con la impresora mediante el puerto paralelo, especifique explícitamente la dirección de entrada o salida de datos (I/O address) de acuerdo con el ajuste del BIOS como `0x378` en `/etc/modprobe.conf`. Si hay dos puertos paralelos cuyas direcciones de entrada o salida son `378` y `278` (hexadecimal), especifique estas últimas como `0x378,0x278`.

Si la interrupción (Interrupt) 7 se encuentra libre, puede activarse con la cadena que se muestra en el Ejemplo 11.1, "/etc/modprobe.conf: Modo de interrupción para el primer puerto paralelo" (p. 266). Antes de activar el modo de interrupción, compruebe si el archivo `/proc/interrupts` ya se está utilizando. Tan sólo aparecen las interrupciones que se utilizan en ese momento. Es posible que esto cambie en función de los componentes de hardware activos. Ningún otro dispositivo debe hacer uso de la interrupción para el puerto paralelo. Si no está seguro, utilice el modo de sondeo mediante `irq=none`.

Ejemplo 11.1 */etc/modprobe.conf: Modo de interrupción para el primer puerto paralelo*

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

11.7.4 Conexiones de impresora de red

Identificación de problemas de red
: Conecte directamente la impresora al equipo. Si desea realizar pruebas, configure la impresora como impresora local. Si esto funciona, los problemas están relacionados con la red.

Comprobación de la red TCP/IP
: La red TCP/IP y la resolución de nombres deben ser funcional.

Comprobación de `lpd` remotos
: Utilice el siguiente comando para comprobar si puede establecerse una conexión TCP como `lpd` (puerto `515`) en *`host`*:

```
netcat -z host 515 && echo ok || echo failed
```

Si la conexión con `lpd` no puede establecerse, es posible que `lpd` no se encuentre activo o que haya problemas básicos de red.

Como usuario `root`, utilice el siguiente comando para consultar un informe de estado (posiblemente muy largo) para *`cola`* en *`host`* remoto, siempre que el `lpd` respectivo se encuentre activo y el host admita consultas:

```
echo -e "\004cola" \
  | netcat -w 2 -p 722 host 515
```

Si `lpd` no responde, es posible que no esté activo o que haya problemas básicos de red. Si `lpd` responde, la respuesta debería mostrar por qué la impresión no es posible en la `cola` en `host`. Si recibe una respuesta como la que aparece en el Ejemplo 11.2, “Mensaje de error desde `lpd`” (p. 267), el problema está causado por el `lpd` remoto.

Ejemplo 11.2 *Mensaje de error desde lpd*

```
lpd: your host does not have line printer access
lpd: queue does not exist
printer: spooling disabled
printer: printing disabled
```

Comprobación de `cupsd` remotos

Por defecto, el servidor de red CUPS debería difundir sus colas cada 30 segundos en puerto UDP `631`. En consecuencia, el siguiente comando puede utilizarse para comprobar si hay un servidor de red CUPS en la red.

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

Si existe una difusión de servidor de red CUPS, aparece la salida como se muestra en el Ejemplo 11.3, “Difusión desde el servidor de red CUPS” (p. 267).

Ejemplo 11.3 *Difusión desde el servidor de red CUPS*

```
ipp://host.domain:631/printers/queue
```

Utilice el siguiente comando para comprobar si puede establecerse una conexión TCP como `lpd` (puerto `631`) en *`host`*:

```
netcat -z host 631 && echo ok || echo failed
```

Si no puede establecerse la conexión con `cupsd`, es posible que `cupsd` no esté activo o que haya problemas básicos de red. `lpstat -h host -l -t` devuelve un informe de estado (posiblemente muy largo) para todas las colas en *`host`*, siempre que el `cupsd` respectivo se encuentre activo y el host admita consultas.

El siguiente comando puede utilizarse para comprobar si la *`cola`* en *`host`* acepta un trabajo de impresión que conste de un solo carácter de retorno de carro. No debería imprimirse nada. Es posible que salga una página en blanco.

```
echo -en "\r" \
  | lp -d queue -h host
```

Solución de problemas de impresoras de red o servidores de impresión dedicados

A veces, los gestores de cola que se ejecutan en un servidor de impresión dedicado pueden ocasionar problemas cuando tienen que hacer frente a muchos trabajos de impresión. Puesto que el gestor de cola del servidor de impresión dedicado es el causante de esto, no hay nada que el usuario pueda hacer. Como solución, eluda el gestor de cola del servidor de impresión dedicado dirigiendo la comunicación a la impresora conectada en el servidor de impresión dedicado directamente a través del zócalo TCP. Consulte la Sección 11.4.2, “Impresoras de red” (p. 254).

De esta forma, la función del servidor de impresión dedicado queda relegada a la de un convertidor de las distintas formas de transferencia de datos (red TCP/IP y conexión de impresora local). Para utilizar este método, necesita saber el puerto TCP del servidor de impresión dedicado. Si la impresora está conectada al servidor de impresión dedicado y encendida, normalmente este puerto TCP puede determinarse con la utilidad `nmap` del paquete `nmap` cierto tiempo después de haber encendido el servidor de impresión dedicado. Por ejemplo, `nmap` *`dirección IP`* puede dar el siguiente resultado para un servidor de impresión dedicado:

```
Port       State       Service
23/tcp     open        telnet
80/tcp     open        http
515/tcp    open        printer
631/tcp    open        cups
9100/tcp   open        jetdirect
```

Esta salida indica que la comunicación con impresora conectada al servidor de impresión dedicado puede realizarse a través del zócalo TCP en el puerto `9100`. Por defecto, `nmap` tan sólo comprueba varios puertos comúnmente conocidos que se enumeran en `/usr/share/nmap/nmap-services`. Para comprobar todos los puertos posibles, utilice el comando `nmap -p` *`de_puerto-a_puerto dirección IP`*. Esto podría llevar cierto tiempo. Para obtener más información, consulte la página Man de `nmap`.

Escriba un comando como:

```
echo -en "\rHello\r\f" | netcat -w 1 IP-address port
cat file | netcat -w 1 IP-address port
```

para enviar directamente cadenas de caracteres o archivos al puerto respectivo para comprobar si puede establecer comunicación con la impresora en este puerto.

11.7.5 Impresión defectuosa sin mensajes de error

El trabajo de impresión finaliza para el sistema de impresión cuando el sistema secundario CUPS completa la transferencia de datos al destinatario (impresora). Si el procesamiento posterior en el destinatario falla (por ejemplo, si la impresora no es capaz de imprimir los datos de la impresora específica), el sistema de impresión no registra este hecho. Si la impresora no es capaz de imprimir los datos específicos de impresora, seleccione un archivo PPD distinto que sea más adecuado para la impresora.

11.7.6 Colas inhabilitadas

Si falla completamente la transferencia de datos al destinatario tras varios intentos, el sistema secundario CUPS, como `usb` o `socket`, informa de un error al sistema de impresión (a `cupsd`). El sistema secundario decide si los intentos tienen sentido hasta que la transferencia de datos se notifica como imposible, y también cuántos intentos han de llevarse a cabo. Puesto que estos intentos se llevarían a cabo en vano, `cupsd` inhabilita la impresión para la cola respectiva. Tras eliminar la causa del problema, el administrador del sistema debe rehabilitar la impresión con el comando `/usr/bin/enable`.

11.7.7 Exploración de CUPS: Supresión de trabajos de impresión

Si un servidor de red CUPS difunde sus colas a los hosts clientes mediante la exploración y se encuentra activo un `cupsd` local adecuado en los hosts clientes, el `cupsd` cliente acepta trabajos de impresión de las aplicaciones y las reenvía al `cupsd` del servidor. Cuando `cupsd` acepta un trabajo de impresión, se le asigna un nuevo número de trabajo. Por lo tanto, el número de trabajo del host cliente difiere del número de trabajo que figura en el servidor. Puesto que, normalmente, un trabajo de impresión se reenvía inmediatamente, no puede suprimirse con el número de trabajo que figura en el host cliente, puesto que el `cupsd` cliente considera el trabajo de impresión como completado al reenviarse al servidor `cupsd`.

Para suprimir un trabajo de impresión que se encuentra en el servidor, utilice un comando como `lpstat -h print-server -o` para determinar el número de trabajo que

figura en el servidor, siempre que éste no haya completado ya el trabajo de impresión (es decir, siempre que no la haya enviado a la impresora). El trabajo de impresión que se encuentra en el servidor puede suprimirse mediante este número de trabajo:

```
cancel -h print-server queue-jobnnumber
```

11.7.8 Trabajos de impresión defectuosos y errores de transferencia de datos

Los trabajos de impresión permanecen en las colas y la impresión se retoma si se apaga la impresora o si el equipo se apaga y rearranca durante el proceso de impresión. Los trabajos de impresión defectuosos pueden eliminarse de la cola mediante `cancel`.

Si un trabajo de impresión es defectuoso o tiene lugar un error en la comunicación entre el host y la impresora, ésta imprime numerosas hojas con caracteres ininteligibles, puesto que no es capaz de procesar los datos correctamente. Para solucionar este problema, proceda como sigue:

1. Para detener la impresión, retire todo el papel de las impresoras de inyección de tinta o abra las bandejas del papel de las impresoras láser. Las impresoras de alta calidad tienen un botón para cancelar la impresión en curso.

2. Es posible que el trabajo de impresión permanezca en cola, puesto que los trabajos tan sólo se eliminan tras haberse enviado completamente a la impresora. Utilice `lpstat -o` o `lpstat -h` *`servidor-de-impresión`* `-o` para comprobar la cola cuya impresión está en curso. Suprima el trabajo de impresión mediante `cancel` *`cola-númerodeimpresión`* o `cancel -h` *`servidor-de-impresión cola-númerodetrabajo`*.

3. Es posible que algunos datos se transfieran a la impresora aun cuando el trabajo de impresión se ha suprimido de la cola. Compruebe si el proceso del sistema secundario CUPS continúa ejecutándose para la cola respectiva y finalícelo. Por ejemplo, para una impresora conectada al puerto paralelo, el comando `fuser -k /dev/lp0` puede utilizarse para finalizar todos los procesos que aún acceden a la impresora (o, en términos más precisos, al puerto paralelo).

4. Restaure completamente la impresora apagándola durante cierto tiempo. A continuación, introduzca el papel y enciéndala.

11.7.9 Depuración del sistema de impresión CUPS

Utilice el procedimiento genérico siguiente para localizar problemas en el sistema de impresión CUPS:

1. Establezca `LogLevel debug` en `/etc/cups/cupsd.conf`.
2. Detenga `cupsd`.
3. Elimine `/var/log/cups/error_log*` para evitar tener que buscar entre archivos de registro muy grandes.
4. Inicie `cupsd`.
5. Repita la acción en la que apareció el problema.
6. Compruebe los mensajes que aparecen en `/var/log/cups/error_log*` para identificar la causa del problema.

11.7.10 Información adicional

Para obtener soluciones para numerosos problemas específicos, consulte la base de datos de asistencia de SUSE en `http://portal.suse.com/`. Realice búsquedas por palabras clave para localizar los artículos pertinentes.

Gestión dinámica de dispositivos de núcleo con udev

12

A partir de la versión 2.6, el núcleo es capaz de añadir o eliminar casi cualquier dispositivo del sistema en ejecución. Los cambios en el estado del dispositivo (si está conectado o se ha eliminado) tienen que propagarse al espacio de usuario. Los dispositivos tienen que configurarse en cuanto se conectan y se descubren. Los usuarios de un dispositivo en concreto deben estar informados acerca de los cambios de estado de este dispositivo. El daemon udev ofrece la infraestructura necesaria para mantener de manera dinámica los archivos del nodo del dispositivo y los enlaces simbólicos en el directorio `/dev`. Asimismo, las reglas de udev proporcionan una forma de conectar las herramientas externas al procesamiento de eventos de los dispositivos de núcleo. De esta forma podrá personalizar la gestión de dispositivos mediante udev, por ejemplo, añadiendo varios guiones para que se ejecuten como parte de la gestión de los dispositivos de núcleo o pidiendo e importando datos adicionales para evaluar durante la gestión de dispositivos.

12.1 Directorio /dev

Los nodos del dispositivo del directorio `/dev` proporcionan acceso a los dispositivos de núcleo correspondientes. Gracias a udev, el directorio `/dev` refleja el estado actual del núcleo. Cada dispositivo de núcleo cuenta con un archivo de dispositivo correspondiente. Si se desconecta un dispositivo del sistema, se eliminará el nodo del dispositivo.

El contenido del directorio `/dev` se conserva en un sistema de archivos temporal, por lo que todos los archivos se crearán de nuevo cada vez que se inicie el sistema. Los archivos creados o modificados manualmente no permanecerán después del rearranque. Los directorios y archivos estáticos que siempre deberían estar presentes en el directorio

/dev sin tener en cuenta el estado del dispositivo de núcleo correspondiente se podrán colocar en el directorio /lib/udev/devices. Al iniciar el sistema, el contenido de ese directorio se copiará en /dev con la misma propiedad y permisos que los archivos de /lib/udev/devices.

12.2 uevents y udev del núcleo

El sistema de archivos sysfs exportará la información del dispositivo necesaria. Por cada dispositivo que el núcleo ha detectado e iniciado, se creará un directorio con el nombre del dispositivo. Contendrá archivos de atributos con propiedades específicas del dispositivo. Cada vez que se añada o se quite un dispositivo, el núcleo enviará un uevent para notificar a udev el cambio.

El daemon udev lee y analiza una vez todas las reglas provenientes de los archivos /etc/udev/rules.d/*.rules al iniciar y los mantiene en memoria. Si los archivos de reglas han cambiado, se han eliminado o se han añadido nuevos, el daemon recibirá un evento y actualizará la representación en memoria de las reglas.

Cada evento recibido se compara con el conjunto de reglas proporcionadas. Las reglas pueden añadir o cambiar las claves de entorno de eventos, pedir un nombre concreto para el nodo del dispositivo que se va a crear, añadir enlaces simbólicos que lleven al nodo o añadir programas para que se ejecuten después de que se cree el nodo del dispositivo. Los uevents del núcleo del controlador provienen de un zócalo de enlace de red del núcleo.

12.3 Controladores, módulos del núcleo y dispositivos

Los controladores del bus del núcleo comprueban la existencia de los dispositivos. Por cada dispositivo detectado, el núcleo crea una estructura de dispositivo interna y el núcleo del controlador envía un uevent al daemon udev. Los dispositivos de bus se identifican mediante un ID con un formato especial que indica el tipo de dispositivo que es. Normalmente estos ID consisten en un ID de proveedor y de producto y otros valores específicos del subsistema. Cada bus cuenta con su propio esquema para estos ID denominado MODALIAS. El núcleo toma la información del dispositivo, compone

una cadena de ID de MODALIAS a partir de él y la envía junto con el evento. En el caso de un ratón USB, tendrá más o menos este aspecto:

```
MODALIAS=usb:v046DpC03Ed2000dc00dsc00dp00ic03isc01ip02
```

Cada controlador del dispositivo lleva una lista de alias conocidos para los dispositivos que puede gestionar. La lista está incluida en el archivo del módulo del núcleo. El programa depmod lee las listas de ID y crea el archivo `modules.alias` en el directorio del núcleo `/lib/modules` para todos los módulos disponibles actualmente. Gracias a esta infraestructura, la carga del módulo es tan sencilla como ejecutar el comando `modprobe` en cada evento que lleve una clave `MODALIAS`. Si se ejecuta `modprobe $MODALIAS`, el alias de dispositivo compuesto para el dispositivo coincidirá con los alias proporcionados por los módulos. Si se encuentra una entrada coincidente, se cargará ese módulo. Será udev el que active este proceso y ocurrirá automáticamente.

12.4 Arranque y configuración inicial del dispositivo

Todos los eventos del dispositivo que se produzcan durante el proceso de arranque antes de que se ejecute el daemon udev se perderán debido a que la infraestructura para gestionar estos eventos se encuentra en el sistema de archivos raíz y no está disponible en ese momento. Para cubrir esta pérdida, el núcleo ofrece un archivo `uevent` para cada dispositivo en el sistema de archivos sysfs. Al escribir `add` en ese archivo, el núcleo volverá a enviar el mismo evento que el que se perdió durante el arranque. Un simple bucle sobre todos los archivos `uevent` en `/sys` activará de nuevo todos los eventos para crear los nodos del dispositivo y realizar la configuración del dispositivo.

Por ejemplo, es posible que la lógica de arranque temprana no inicialice un ratón USB presente durante el arranque debido a que el controlador no estaba disponible en ese momento. Se ha perdido el evento encargado del descubrimiento del dispositivo y se ha producido un error al encontrar un módulo del núcleo para el dispositivo. En lugar de buscar manualmente dispositivos conectados, udev sólo solicitará todos los eventos del dispositivo desde el núcleo después de que esté disponible el sistema de archivos raíz, de manera que el evento para el ratón USB se ejecutará de nuevo. Ahora encontrará el módulo del núcleo en el sistema de archivos raíz montado, por lo que el ratón USB podrá inicializarse.

Desde el espacio de usuario, no hay una diferencia visible entre la secuencia de coldplug de dispositivo y el descubrimiento de dispositivos durante el tiempo de ejecución. En ambos casos, se usarán las mismas reglas para que coincidan y se ejecutan los mismos programas configurados.

12.5 Depuración de los eventos udev

Se puede usar el programa `udevmonitor` para ver los eventos del núcleo del controlador y la coordinación de los procesos del evento udev.

```
UEVENT[1132632714.285362] add@/devices/pci0000:00/0000:00:1d.1/usb2/2-2
UEVENT[1132632714.288166] add@/devices/pci0000:00/0000:00:1d.1/usb2/2-2/2-2:1.0
UEVENT[1132632714.309485] add@/class/input/input6
UEVENT[1132632714.309511] add@/class/input/input6/mouse2
UEVENT[1132632714.309524] add@/class/usb_device/usbdev2.12
UDEV  [1132632714.348966] add@/devices/pci0000:00/0000:00:1d.1/usb2/2-2
UDEV  [1132632714.420947] add@/devices/pci0000:00/0000:00:1d.1/usb2/2-2/2-2:1.0
UDEV  [1132632714.427298] add@/class/input/input6
UDEV  [1132632714.434223] add@/class/usb_device/usbdev2.12
UDEV  [1132632714.439934] add@/class/input/input6/mouse2
```

Las líneas `UEVENT` muestran los eventos que el núcleo ha enviado por el enlace de red. Las líneas `UDEV` muestran los gestores de los eventos udev finalizados. La sincronización se muestra en microsegundos. El tiempo que pasa entre `UEVENT` y `UDEV` se corresponde con el tiempo que udev necesitó para procesar este evento, o bien se ha retrasado la ejecución del daemon udev para sincronizar este evento con eventos relacionados y en ejecución. Por ejemplo, los eventos para las particiones de disco duro siempre esperan a que el evento del dispositivo del disco principal finalice, ya que los eventos de particiones pueden confiar en los datos del evento que el evento del disco principal ha consultado en el hardware.

`udevmonitor --env` muestra el entorno de eventos completo:

```
UDEV  [1132633002.937243] add@/class/input/input7
UDEV_LOG=3
ACTION=add
DEVPATH=/class/input/input7
SUBSYSTEM=input
SEQNUM=1043
PHYSDEVPATH=/devices/pci0000:00/0000:00:1d.1/usb2/2-2/2-2:1.0
PHYSDEVBUS=usb
PHYSDEVDRIVER=usbhid
PRODUCT=3/46d/c03e/2000
NAME="Logitech USB-PS/2 Optical Mouse"
PHYS="usb-0000:00:1d.1-2/input0"
```

```
UNIQ=""
EV=7
KEY=70000 0 0 0 0 0 0 0 0
REL=103
```

udev también envía mensajes a syslog. La prioridad por defecto de syslog que controla los mensajes enviados a syslog está especificada en el archivo de configuración de udev `/etc/udev/udev.conf`. La prioridad del registro del daemon en ejecución puede cambiarse con `udevcontrol log_priority=`*`nivel/número`*.

12.6 Influencia de la gestión de eventos de dispositivo del núcleo con reglas de udev

Una regla udev puede coincidir con cualquier propiedad que el núcleo añada al evento en sí mismo o con cualquier información que el núcleo exporte a `sysfs`. La regla también puede pedir información adicional desde programas externos. Cada evento se contrasta con todas las reglas proporcionadas. Las reglas se encuentran en el directorio `/etc/udev/rules.d`.

Cada línea del archivo de reglas contiene al menos un par de valores clave. Existen dos clases de claves: de coincidencia y de asignación. Si todas las claves de coincidencia concuerdan con sus valores, se aplicará la regla y las claves de asignación se asignarán al valor especificado. Una regla de coincidencia puede especificar el nombre del nodo del dispositivo, añadir enlaces simbólicos que apunten al nodo o ejecutar un programa especificado como parte de la gestión de eventos. Si no se encuentra ninguna regla coincidente, se utilizará el nombre del nodo del dispositivo por defecto para crear el nodo del dispositivo. La sintaxis de la regla y las claves proporcionadas para coincidir o importar datos se describen en la página Man de udev.

12.7 Denominación permanente de dispositivos

El directorio dinámico de dispositivos y la infraestructura de reglas de udev hacen posible poder dar nombres estables a todos los dispositivos de disco, sin tener en cuenta

el orden de reconocimiento o la conexión utilizada para conectar el dispositivo. Todos los dispositivos de bloque adecuados que el núcleo crea es examinado por herramientas con conocimientos especiales acerca de algunos buses, tipos de unidad o sistemas de archivos. Además del nombre dinámico del nodo del dispositivo proporcionado por el núcleo, udev mantiene tipos de enlaces simbólicos permanentes apuntando al dispositivo:

```
/dev/disk
|-- by-id
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B -> ../../sda
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part1 -> ../../sda1
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part6 -> ../../sda6
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part7 -> ../../sda7
|   |-- usb-Generic_STORAGE_DEVICE_02773 -> ../../sdd
|   `-- usb-Generic_STORAGE_DEVICE_02773-part1 -> ../../sdd1
|-- by-label
|   |-- Photos -> ../../sdd1
|   |-- SUSE10 -> ../../sda7
|   `-- devel -> ../../sda6
|-- by-path
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0 -> ../../sda
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part1 -> ../../sda1
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part6 -> ../../sda6
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part7 -> ../../sda7
|   |-- pci-0000:00:1f.2-scsi-1:0:0:0 -> ../../sr0
|   |-- usb-02773:0:0:2 -> ../../sdd
|   |-- usb-02773:0:0:2-part1 -> ../../sdd1
`-- by-uuid
    |-- 159a47a4-e6e6-40be-a757-a629991479ae -> ../../sda7
    |-- 3e999973-00c9-4917-9442-b7633bd95b9e -> ../../sda6
    `-- 4210-8F8C -> ../../sdd1
```

12.8 Paquete hotplug sustituido

El paquete hotplug utilizado anteriormente se ha sustituido completamente por la infraestructura de udev y del núcleo relacionado con udev. Las partes siguientes de la anterior infraestructura de hotplug se han vuelto obsoletas o udev ha asumido sus funciones:

`/etc/hotplug/*.agent`
: Ya no es necesario o se ha movido a `/lib/udev`.

`/etc/hotplug/*.rc`
: Sustituido por la activación de `/sys/*/uevent`.

`/etc/hotplug/blacklist`
: Sustituido por la opción de lista negra (`blacklist`) de `modprobe.conf`.

`/etc/dev.d/*`
: Sustituido por la clave `RUN` de la regla udev.

`/etc/hotplug.d/*`
: Sustituido por la clave `RUN` de la regla udev.

`/sbin/hotplug`
: Sustituido por la escucha de udevd en el enlace de red. Sólo se usa en el sistema de archivos RAM inicial hasta que puede montarse el sistema de archivos raíz. Después se inhabilita.

`/dev/*`
: Sustituido por udev dinámico y el contenido estático de `/lib/udev/devices/*`.

Los archivos y directorios siguientes contienen los elementos cruciales de la infraestructura de udev:

`/etc/udev/udev.conf`
: Archivo de configuración principal de udev.

`/etc/udev/rules.d/*`
: Reglas coincidentes de eventos de udev.

`/lib/udev/devices/*`
: Contenido estático de `/dev`.

`/lib/udev/*`
: Programas de ayudantes que las reglas de udev han llamado.

12.9 Información adicional

Para obtener más información acerca de la infraestructura de udev, consulte las páginas Man siguientes:

udev
: Información general acerca de udev, claves y reglas, además de otras cuestiones sobre configuración importantes.

udevinfo
: udevinfo puede usarse para consultar la información del dispositivo desde la base de datos de udev.

udevd
: Información acerca del daemon de gestión de eventos de udev.

udevmonitor
: udevmonitor imprime el núcleo y la secuencia de eventos de udev en la consola. Esta herramienta se utiliza principalmente para tareas de depuración.

13 Sistemas de archivos en Linux

Linux es compatible con varios sistemas de archivos distintos. Este capítulo presenta una breve descripción general de los sistemas de archivos de Linux más populares, con especial dedicación a sus conceptos de diseño, ventajas y campos de aplicación. Se proporciona además información adicional acerca de LFS (compatibilidad para archivos grandes) en Linux.

13.1 Terminología

metadatos
: Estructura de datos interna de un sistema de archivos que garantiza que todos los datos del disco están bien organizados y se puede acceder a ellos correctamente. En esencia, se trata de "datos acerca de los datos". Casi todos los sistemas de archivos cuentan con una estructura de metadatos propia, que constituye uno de los motivos por los que los sistemas de archivos presentan características de funcionamiento distintas. Resulta extremadamente importante mantener los metadatos intactos; si no, podría ser imposible acceder a todos los datos del sistema de archivos.

inodo
: Elemento que contiene diversa información acerca de un archivo, entre la que se incluye su tamaño, el número de enlaces, los punteros a los bloques del disco donde está almacenado realmente el contenido del archivo, así como la fecha y la hora de creación, modificación y acceso.

diario

En el contexto de un sistema de archivos, un diario es una estructura del disco que contiene un tipo de registro en el que el sistema de archivos almacena lo que está a punto de cambiar en los metadatos del sistema de archivos. La anotación en este registro reduce en gran medida el tiempo de recuperación de los sistemas Linux, ya que deja de ser necesario efectuar el lento proceso de búsqueda para comprobar todo el sistema de archivos en el inicio del sistema. En su lugar, sólo se vuelve a comprobar el diario.

13.2 Sistemas de archivos de Linux principales

Al contrario de lo que ocurría hace dos o tres años, la elección de un sistema de archivos para un sistema Linux ha dejado de ser un proceso de unos cuantos segundos (en el que se elegía entre Ext2 o ReiserFS). Los núcleos a partir de la versión 2.4 ofrecen distintos sistemas de archivos entre los que elegir. A continuación se ofrece una descripción general del modo de funcionamiento básico de esos sistemas de archivos y las ventajas que ofrecen.

Es muy importante recordar que puede no haber un sistema de archivos que sea el más indicado para todos los tipos de aplicaciones. Cada uno presenta ventajas y puntos débiles propios que deben tenerse en cuenta. Incluso los sistemas de archivos más sofisticados no pueden reemplazar, por ejemplo, a una buena estrategia de copias de seguridad.

Los términos *integridad de los datos* y *coherencia de los datos,* cuando aparecen en este capítulo, no hacen referencia a la coherencia de los datos del espacio del usuario (los que las aplicaciones escriben en los archivos correspondientes). La coherencia de esos datos deben controlarla las propias aplicaciones.

IMPORTANTE: Configuración de sistemas de archivos

A menos que se indique lo contrario en este capítulo, todos los pasos necesarios para configurar o cambiar particiones y sistemas de archivos se pueden realizar desde YaST.

13.2.1 ReiserFS

La que es oficialmente una de las funciones clave de la versión de núcleos 2.4, ReiserFS, ha estado disponible como parche para los núcleos de SUSE 2.2.x desde la versión 6.4 de SUSE Linux. ReiserFS fue diseñado por Hans Reiser y el equipo de desarrollo Namesys. Ha demostrado ser una potente alternativa para Ext2. Sus ventajas principales son una mejor utilización del espacio del disco, un mejor rendimiento en el acceso al disco y una recuperación más rápida tras las caídas del sistema.

Las ventajas de ReiserFS, con más detalle, son:

Mejor utilización del espacio del disco
: En ReiserFS, todos los datos se organizan en una estructura llamada B*-balanced tree (árbol equilibrado). La estructura en árbol contribuye a la mejor utilización del espacio del disco debido a que los archivos pequeños se pueden almacenar directamente en los nodos de hojas del árbol B* en lugar de almacenarse en otro lugar y mantener únicamente un puntero a la ubicación real en el disco. Además, el almacenamiento no se asigna en unidades de 1 o 4 kB, sino en porciones del tamaño exacto necesario. Otro beneficio reside en la asignación dinámica de inodos. De esta forma el sistema de archivos resulta más flexible que los sistemas tradicionales, como Ext2, donde la densidad de inodos se debe especificar en el momento en que se crea el sistema de archivos.

Mejor rendimiento en el acceso al disco
: En el caso de los archivos pequeños, tanto los datos de los archivos como la información (inodo) “stat_data” se almacenan a menudo unos al lado de la otra. Se pueden leer con una sola operación de E/S del disco, lo que significa que sólo es necesario acceder al disco una vez para recuperar toda la información necesaria.

Recuperación rápida tras las caídas del sistema
: Mediante un diario en el que se realiza un seguimiento de los cambios recientes en los metadatos, se puede realizar una comprobación del sistema en cuestión de segundos, incluso en sistemas de archivos de gran tamaño.

Fiabilidad gracias al registro de datos
: ReiserFS es compatible también con el registro de datos en un diario y con los modos de ordenación de datos similares a los conceptos descritos en la sección de Ext3, Sección 13.2.3, “Ext3” (p. 285). El modo predeterminado es `data=ordered`, el cual garantiza la integridad tanto de los datos como de los metadatos y se utiliza el registro en el diario sólo con los metadatos.

13.2.2 Ext2

Los orígenes de Ext2 se remontan a los primeros días de la historia de Linux. Su predecesor, el sistema de archivos extendido (Extended File System), se implantó en abril de 1992 y se integró en Linux 0.96c. El sistema de archivos extendido experimentó diversas modificaciones y, como Ext2, se convirtió en el sistema de archivos para Linux más popular durante años. Con la creación de los sistemas de archivos con registro en diario y sus sorprendentemente cortos tiempos de recuperación, Ext2 perdió protagonismo.

Un breve resumen de las ventajas de Ext2 puede ayudar a entender por qué fue, y sigue siendo en algunos casos, el sistema de archivos favorito de muchos usuarios de Linux.

Solidez
: Dado que es un “veterano”, Ext2 ha sido sometido a muchas mejoras y probado en profundidad. Puede que ésa sea la razón por la que se hace referencia a él como una roca sólida. Cuando, tras un fallo del sistema, no es posible desmontar el sistema de archivos limpiamente, e2fsck comienza a analizar los datos del sistema de archivos. Los metadatos recuperan un estado coherente y los archivos o bloques de datos pendientes se escriben en un directorio designado (denominado `lost +found`, es decir, "objetos perdidos"). Al contrario de lo que ocurre con los sistemas de archivos con registro en diario, e2fsck analiza todo el sistema de archivos y no sólo los bits de metadatos modificados recientemente. Este proceso consume mucho más tiempo que la comprobación del registro en un sistema de archivos con diario. Según el tamaño del sistema de archivos, puede suponer media hora o más. Por tanto, no es aconsejable elegir Ext2 para un servidor que requiera un alto grado de disponibilidad. Sin embargo, dado que Ext2 no mantiene ningún diario y emplea sensiblemente menos memoria, a veces resulta más rápido que otros sistemas de archivos.

Fácil actualización
: El código de Ext2 es la base firme sobre la que Ext3 pudo convertirse en un sistema de archivos de última generación muy aclamado. Su fiabilidad y solidez se combinaron elegantemente con las ventajas de un sistema de archivos con registro en diario.

13.2.3 Ext3

Ext3 fue concebido por Stephen Tweedie. A diferencia de todos los demás sistemas de archivos de última generación, Ext3 no parte de un principio de diseño completamente nuevo, sino que está basado en Ext2. Ambos sistemas de archivos están estrechamente vinculados. Un sistema de archivos Ext3 se puede montar fácilmente sobre un sistema de archivos Ext2. La diferencia fundamental entre ambos es que Ext3 es compatible también con el registro en diario. En resumen, Ext3 presenta tres ventajas principales:

Actualización sencilla y muy fiable de Ext2
: Dado que Ext3 está basado en el código de Ext2 y comparte los mismos formatos para el disco y los metadatos, la actualización de Ext2 a Ext3 resulta increíblemente fácil. Al contrario que las transiciones a otros sistemas de archivos con registro en diario, como ReiserFS o XFS, que pueden ser bastante tediosas (con la necesidad de hacer copias de seguridad de todo el sistema de archivos para volver a crearlo desde cero), el cambio a Ext3 se lleva a cabo en cuestión de minutos. También es un proceso muy seguro, ya que volver a generar todo un sistema de archivos desde cero puede presentar problemas. Si se tiene en cuenta la cantidad de sistemas Ext2 disponibles que esperan una actualización a un sistema de archivos con diario, es fácil imaginar la importancia que puede tener Ext3 para muchos administradores de sistemas. El cambio de Ext3 a Ext2 es tan fácil como la actualización en sentido contrario. Basta con desmontar el sistema de archivos Ext3 y volver a montarlo como sistema de archivos Ext2.

Fiabilidad y rendimiento
: Algunos de los sistemas de archivos con registro en diario siguen el principio de "sólo metadatos" en el registro. Esto significa que los metadatos conservan siempre un estado coherente, lo que no se puede garantizar directamente para los propios datos del sistema de archivos. Ext3 está diseñado para ocuparse tanto de los metadatos como de los datos. El nivel de "ocupación" se puede personalizar. Si se habilita Ext3 en el modo `data=journal`, se consigue la máxima seguridad (integridad de los datos), pero se puede ralentizar el sistema, ya que se registran en el diario tanto los metadatos como los datos. Un concepto relativamente nuevo consiste en utilizar el modo `data=ordered`, el cual garantiza la integridad tanto de los datos como de los metadatos, pero utiliza el registro en el diario sólo con los metadatos. El controlador del sistema de archivos recopila todos los bloques de datos que corresponden a una actualización de los metadatos. Estos bloques de datos se escriben en el disco antes de que se actualicen los metadatos. Como resultado, se consigue la coherencia tanto de los metadatos como de los datos sin

sacrificar el rendimiento. Una tercera opción consiste en utilizar `data=writeback`, que permite que los datos se escriban en el sistema de archivos principal después de que los metadatos correspondientes se hayan consignado en el diario. Esta opción se considera a menudo la mejor en términos de rendimiento. Sin embargo, puede ocurrir que vuelvan a aparecer datos obsoletos en los archivos después de una caída y recuperación del sistema, al tiempo que se mantiene la integridad interna del sistema de archivos. Mientras no se especifique otra cosa, Ext3 se ejecuta con el valor por defecto `data=ordered`.

13.2.4 Conversión de un sistema de archivos Ext2 a Ext3

Para convertir un sistema de archivos Ext2 a Ext3, haga lo siguiente:

1. Cree un diario de Ext3 ejecutando `tune2fs -j` como usuario Root. De este modo se crea un diario Ext3 con los parámetros por defecto.

   Para decidir el tamaño del diario y el dispositivo en el que debe residir, ejecute `tune2fs -J` junto con las opciones de diario que desee: `size=` y `device=`. Puede encontrar más información acerca del programa tune2fs en la página de manual de tune2fs.

2. Para asegurarse de que el sistema de archivos Ext3 se reconoce como tal, edite el archivo `/etc/fstab` como usuario Root, cambie el tipo del sistema de archivos especificado para la partición correspondiente de `ext2` a `ext3`. El cambio surte efecto tras el siguiente rearranque.

3. Para arrancar una configuración de sistema de archivos raíz como partición Ext3, incluya los módulos `ext3` y `jbd` en `initrd`. Para ello, edite `/etc/sysconfig/kernel` como usuario Root y añada `ext3` y `jbd` a la variable `INITRD_MODULES`. Tras guardar los cambios, ejecute el comando `mkinitrd`. De este modo se genera un nuevo initrd y se prepara para su uso.

13.2.5 Reiser4

Justo después de que apareciera en el mercado el núcleo 2.6, la familia de sistemas de archivos con registro en diario se amplió con un nuevo miembro: Reiser4. Reiser4 es

esencialmente distinto de su predecesor, ReiserFS (versión 3.6). Introduce el concepto de complementos para aumentar la funcionalidad del sistema de archivos, así como un concepto de seguridad muy avanzado.

Concepto de seguridad avanzado
: Al diseñar Reiser4, los desarrolladores hicieron hincapié en la implantación de funciones relativas a la seguridad. Por tanto, Reiser4 se presenta con un conjunto de complementos destinados a la seguridad. El más importante de ellos introduce el concepto de "elementos" de archivo. En la actualidad, los controles de acceso a archivos están definidos por archivo. Si se cuenta con un archivo grande que incluye información pertinente para varios usuarios, grupos o aplicaciones, los derechos de acceso deben ser lo suficientemente imprecisos para que puedan incluir a todas las partes involucradas. Reiser4 permite dividir ese tipo de archivos en partes más pequeñas, conocidas como "elementos". Así, los derechos de acceso se pueden definir para cada elemento y cada usuario de forma independiente, lo que permite una gestión mucho más precisa de la seguridad de los archivos. Un ejemplo perfecto es `/etc/passwd`. Hasta ahora, sólo podían leer y editar este archivo los usuarios `Root`, mientras que, los que no lo fueran sólo obtenían acceso de lectura al archivo. Mediante el concepto de elemento de Reiser4, se puede dividir el archivo en un conjunto de elementos (uno por usuario) y permitir a los usuarios o las aplicaciones modificar sus propios datos, pero no acceder a los datos de otros usuarios. Este concepto supone una mejora tanto de la seguridad como de la flexibilidad.

Ampliabilidad a través de complementos
: Muchas de las funciones del sistema de archivos y de las funciones externas que emplea normalmente un sistema de archivos se implantan como complementos en Reiser4. Estos complementos se pueden añadir fácilmente al sistema base, por lo que desaparece la necesidad de volver a compilar el núcleo o formatear el disco duro para añadir nuevas funciones al sistema de archivos.

Mejor disposición del sistema de archivos a través de la asignación retardada
: Al igual que XFS, Reiser4 es compatible con la asignación retardada. Consulte la Sección 13.2.6, "XFS" (p. 287). El uso de la asignación retardada incluso para los metadatos puede resultar en una disposición general más adecuada.

13.2.6 XFS

Pensado en un principio como sistema de archivos para su sistema operativo IRIX, SGI inició el desarrollo de XFS a principios de la década de 1990. La idea subyacente en

XFS era la de crear un sistema de archivos con registro en diario de 64 bits de alto rendimiento para afrontar los grandes retos de la informática actual. XFS es muy bueno a la hora de manipular archivos grandes y ofrece un rendimiento adecuado en hardware de alta tecnología. Con todo, incluso XFS presenta alguna desventaja. Como ReiserFS, XFS pone mucha atención a la integridad de los metadatos, pero menos a la de los datos.

Si se revisan rápidamente las funciones clave de XFS, se entiende el motivo por el que puede constituir un serio competidor para otros sistemas de archivos con registro en diario en informática de alta tecnología.

Gran escalabilidad a través de grupos de asignación
: En el momento en que se crea un sistema de archivos XFS, el dispositivo de bloqueo subyacente se divide en ocho o más regiones lineales del mismo tamaño. Estas regiones se conocen como *grupos de asignación*. Cada grupo de asignación gestiona los inodos y el espacio libre en el disco propios. En la práctica, los grupos de asignación se pueden considerar como sistemas de archivos dentro de un sistema de archivos. Dado que los grupos de asignación son bastante independientes entre sí, el núcleo puede acceder a más de uno a la vez, lo que constituye la clave de la gran escalabilidad de XFS. Obviamente, el concepto de grupos de asignación independientes satisface las necesidades de los sistemas con varios procesadores.

Alto rendimiento mediante la gestión eficaz del espacio del disco
: El espacio libre y los inodos se gestionan mediante árboles B^+ dentro de los grupos de asignación. El uso de árboles B^+ contribuye en gran medida a aumentar el rendimiento y la escalabilidad de XFS. XFS emplea *asignación retardada:* gestiona la asignación dividiendo el proceso en dos partes. La transacción pendiente se almacena en RAM y se reserva la cantidad de espacio adecuada. XFS no decide en ese momento el lugar exacto (hablando de bloques del sistema de archivos) donde se deben almacenar los datos. Esta decisión se retarda hasta el último momento posible. Algunos datos temporales de corta duración pueden no llegar al disco nunca, porque pueden haber quedado obsoletos para el momento en que XFS decide dónde guardarlos. Así, XFS aumenta el rendimiento en la escritura y reduce la fragmentación del sistema de archivos. Debido a que la asignación retardada tiene como resultado menos eventos de escritura que en otros sistemas de archivos, es probable que la pérdida de datos tras una caída del sistema durante un proceso de escritura sea más grave.

Asignación previa para evitar la fragmentación del sistema de archivos
: Antes de escribir los datos en el sistema de archivos, XFS *reserva* (realiza una asignación previa) el espacio libre necesario para un archivo, con lo que se reduce

en gran medida la fragmentación del sistema de archivos. El rendimiento aumenta dado que el contenido de cada archivo no está distribuido por todo el sistema de archivos.

13.3 Otros sistemas de archivos compatibles

La Tabla 13.1, "Tipos de sistemas de archivos en Linux" (p. 289) resume otros sistemas de archivos compatibles con Linux. Estos sistemas se admiten principalmente para asegurar la compatibilidad y el intercambio de datos en distintos tipos de medios o de sistemas operativos distintos.

Tabla 13.1 *Tipos de sistemas de archivos en Linux*

`cramfs`	*Compressed ROM File System:* sistema de archivos comprimido de sólo lectura para ROM.
`hpfs`	*High Performance File System:* sistema de archivos estándar para IBM OS/2 que se admite en modo de sólo lectura únicamente.
`iso9660`	Sistema de archivos estándar para discos CD-ROM.
`minix`	Este sistema de archivos tuvo su origen en proyectos académicos sobre sistemas operativos y fue el primer sistema de archivos utilizado en Linux. En la actualidad, se utiliza en los disquetes.
`msdos`	*fat,* sistema de archivos usado originalmente en DOS que en la actualidad se emplea en diversos sistemas operativos.
`ncpfs`	Sistema de archivos para montar volúmenes de Novell en redes.
`nfs`	*Network File System:* este sistema de archivos permite almacenar los datos en cualquier equipo de una red y se puede otorgar acceso a ellos a través de una red.

`smbfs`	*Server Message Block File System* se emplea en productos como Windows para habilitar el acceso a los archivos a través de una red.
`sysv`	Se utiliza en SCO UNIX, Xenix y Coherent (sistemas comerciales de UNIX para equipos PC).
`ufs`	Se utiliza en BSD, SunOS y NeXTstep. Se admite únicamente en modo de sólo lectura.
`umsdos`	*UNIX on MSDOS:* aplicado sobre un sistema de archivos `fat` normal, proporciona la funcionalidad de UNIX (permisos, enlaces, nombres de archivo largos) gracias a la creación de archivos especiales.
`vfat`	*Virtual FAT:* extensión del sistema de archivos `fat` (compatible con nombres de archivos largos).
`ntfs`	*Windows NT File System*, de sólo lectura.

13.4 Compatibilidad con archivos grandes en Linux

En su origen, Linux sólo admitía 2 GB como tamaño de archivo máximo. Esto era suficiente antes de la explosión multimedia y siempre que nadie intentara manipular enormes bases de datos en Linux. Al ser cada vez más importante en el entorno de la informática de servidores, el núcleo y la biblioteca C se modificaron para que admitieran tamaños superiores a los 2 GB al utilizar un nuevo conjunto de interfaces que debían emplear las aplicaciones. En la actualidad, casi todos los sistemas de archivos principales ofrecen compatibilidad con LFS, lo que permite realizar tareas informáticas de alto nivel. La Tabla 13.2, “Tamaños máximos de sistemas de archivos (formato de disco)” (p. 291) presenta una visión general de las limitaciones actuales de los archivos y sistemas de archivos de Linux.

Tabla 13.2 *Tamaños máximos de sistemas de archivos (formato de disco)*

Sistema de archivos	Tamaño de archivo (Bytes)	Tamaño de sistema de archivos (Bytes)
Ext2 o Ext3 (tamaño de bloque de 1 kB)	2^{34} (16 GB)	2^{41} (2 TB)
Ext2 o Ext3 (tamaño de bloque de 2 kB)	2^{38} (256 GB)	2^{43} (8 TB)
Ext2 o Ext3 (tamaño de bloque de 4 kB)	2^{41} (2 TB)	2^{43}-4096 (16 TB-4096 Bytes)
Ext2 o Ext3 (tamaño de bloque de 8 kB) (sistemas con páginas de 8 kB, como Alpha)	2^{46} (64 TB)	2^{45} (32 TB)
ReiserFS v3	2^{46} (64 TB)	2^{45} (32 TB)
XFS	2^{63} (8 EB)	2^{63} (8 EB)
NFSv2 (cliente)	2^{31} (2 GB)	2^{63} (8 EB)
NFSv3 (cliente)	2^{63} (8 EB)	2^{63} (8 EB)

IMPORTANTE: Límites del núcleo de Linux

La Tabla 13.2, “Tamaños máximos de sistemas de archivos (formato de disco)” (p. 291) describe las limitaciones en relación con el formato de disco. El núcleo 2.6 impone sus propios límites en el tamaño de los archivos y los sistemas de archivos que gestiona. Esos límites son los siguientes:

Tamaño de archivo
: En sistemas de 32 bits, los archivos no pueden superar un tamaño de 2 TB (2^{41} bytes).

Tamaño de sistema de archivos
: Los sistemas de archivos pueden tener un tamaño máximo de 2^{73} bytes. Sin embargo, este límite no lo pueden alcanzar todavía los componentes de hardware disponibles en la actualidad.

13.5 Información adicional

Cada uno de los proyectos de sistemas de archivos descritos arriba tiene su propia página Web en la que se puede encontrar información sobre listas de correo, documentación adicional o secciones de preguntas más frecuentes.

- `http://e2fsprogs.sourceforge.net/`
- `http://www.zipworld.com.au/~akpm/linux/ext3/`
- `http://www.namesys.com/`
- `http://oss.software.ibm.com/developerworks/opensource/jfs/`
- `http://oss.sgi.com/projects/xfs/`

Está disponible además un completo tutorial acerca de los sistemas de archivos de Linux en *IBM developerWorks:* `http://www-106.ibm.com/developerworks/library/l-fs.html`. Si desea ver una comparación de los distintos sistemas de archivos con registro en diario en Linux, consulte el artículo de Juan I. Santos Florido en *Linuxgazette:* `http://www.linuxgazette.com/issue55/florido.html`. Quienes estén interesados en consultar un análisis en profundidad de LFS en Linux, deberían visitar el sitio sobre LFS de Andreas Jaeger: `http://www.suse.de/~aj/linux_lfs.html`.

14 El sistema X Window

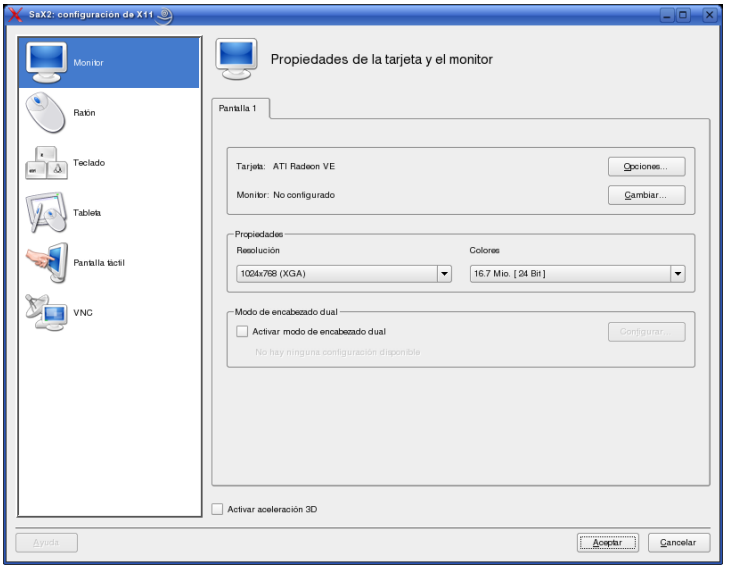
El sistema X Window (X11) es el estándar de facto para las interfaces gráficas de usuario en UNIX. X está basado en red, lo que permite que las aplicaciones iniciadas en un host se muestren en otro host conectado mediante cualquier tipo de red (LAN o Internet). En este capítulo se describe la configuración y la optimización del entorno del sistema X Window, se ofrece información general sobre el uso de fuentes en SUSE Linux y se explica la configuración de OpenGL y 3D.

El texto siguiente contiene varias referencias a la documentación que se puede encontrar en `/usr/share/doc/packages/Xorg` y en `/usr/share/doc/howto/es`. Este material, junto a sus respectivas páginas de manual, sólo estará disponible si se instalan los paquetes de documentación apropiados (`xorg-x11-doc`, `xorg-x11-man` y `howtoenh`).

14.1 Configuración de X11 con SaX2

La interfaz gráfica de usuario, o el servidor X, gestiona la comunicación entre el hardware y el software. Los escritorios, como KDE y GNOME, y la gran variedad de gestores de ventanas utilizan el servidor X para interactuar con el usuario. La interfaz gráfica de usuario se configura durante la instalación. Para cambiar la configuración más adelante, utilice el correspondiente módulo del Centro de control de YaST o ejecute SaX2 manualmente desde la línea de comando mediante el comando `sax2`. La ventana principal de SaX2 ofrece una interfaz común para todos los módulos individuales del Centro de control de YaST.

Figura 14.1 *Ventana principal de SaX2*



En la barra de navegación situada a la izquierda, existen seis elementos y cada uno de ellos muestra el correspondiente cuadro de diálogo de configuración del Centro de control de YaST. La secciones anteriormente mencionadas se encuentran en el Capítulo *Configuración del sistema con YaST* (↑Inicio).

Monitor
: Para obtener una descripción de la configuración de la tarjeta gráfica y de monitor, consulte la Sección “Propiedades de la tarjeta y el monitor” (Capítulo 2, *Configuración del sistema con YaST*, ↑Inicio).

Ratón
: Para obtener una descripción de la configuración del ratón en el entorno gráfico, consulte la Sección “Propiedades del ratón” (Capítulo 2, *Configuración del sistema con YaST*, ↑Inicio).

Teclado
: Para obtener una descripción de la configuración del teclado en el entorno gráfico, consulte la Sección “Propiedades del teclado” (Capítulo 2, *Configuración del sistema con YaST*, ↑Inicio).

Tableta
: Para obtener una descripción de la configuración de la tableta gráfica, consulte la Sección “Propiedades de la tableta” (Capítulo 2, *Configuración del sistema con YaST*, ↑Inicio).

Pantalla táctil
: Para obtener una descripción de la configuración de la pantalla táctil, consulte la Sección “Propiedades de la pantalla táctil” (Capítulo 2, *Configuración del sistema con YaST*, ↑Inicio).

VNC
: Para obtener una descripción de la configuración de VNC, consulte la Sección “Propiedades de acceso remoto” (Capítulo 2, *Configuración del sistema con YaST*, ↑Inicio).

14.2 Optimización de la configuración de X

X.Org es una implementación de código abierto del sistema X Window. Lo desarrolla la X.Org Foundation, que es responsable también de desarrollar nuevas tecnologías y estándares para el sistema X Window.

Para sacar el máximo partido al hardware disponible (el ratón, la tarjeta gráfica, el monitor y el teclado, entre otros), se puede optimizar manualmente la configuración. A continuación se explican algunos aspectos de dicha optimización. Para obtener información detallada sobre la configuración del sistema X Window, consulte los diferentes archivos del directorio `/usr/share/doc/packages/Xorg` así como `man xorg.conf`.

AVISO

Tenga mucha precaución a la hora de configurar el sistema X Window. No inicie jamás el sistema X Window hasta haber completado la configuración. Un sistema mal configurado puede provocar daños irreparables en el hardware (en particular, en los monitores de frecuencia fija). Ni los autores de este libro ni SUSE Linux pueden considerarse responsables de tales daños. La información que se ofrece ha sido cuidadosamente contrastada, pero no se garantiza que

todos los métodos aquí expuestos sean correctos ni que no vayan a dañar su hardware.

Los programas SaX2 y xorgconfig crean el archivo `xorg.conf`, por defecto en `/etc/X11`. Éste es el archivo principal de configuración del sistema X Window. Aquí se encuentran los ajustes referentes a la tarjeta gráfica, el ratón y el monitor.

A continuación se describe la estructura del archivo de configuración `/etc/X11/xorg.conf`. Este archivo se compone de diferentes secciones, cada una de las cuales hace referencia a un aspecto determinado de la configuración. Cada sección comienza con la palabra clave `Section <nombre>` y termina con `EndSection`. Las secciones tienen la siguiente forma:

```
Section nombre
  entrada 1
  entrada 2
  entrada n
EndSection
```

Los tipos de sección disponibles aparecen en la Tabla 14.1, “Secciones de /etc/X11/xorg.conf” (p. 296).

Tabla 14.1 *Secciones de /etc/X11/xorg.conf*

Tipo	Significado
`Files`	Esta sección describe las vías que se utilizan para las fuentes y la tabla de colores RGB.
`ServerFlags`	Aquí se establecen las opciones generales.
`InputDevice`	En esta sección se configuran los dispositivos de entrada, tales como teclados y dispositivos de entrada especiales (touchpads, joysticks etc.). Los parámetros más importantes de esta sección son `Driver` y las opciones que definen `Protocol` y `Device`.
`Monitor`	Describe el monitor que se utiliza. Los elementos de esta sección son un nombre, al que más adelante hace referencia la definición `Screen`, `bandwidth` y los límites de frecuencia de sincronización (`HorizSync` y `VertRefresh`). Los ajustes se establecen en MHz, kHz y Hz. Normalmente, el servidor rechaza

Tipo	Significado
	las modelines que no se correspondan con las características del monitor. Esto evita que se envíen por error al monitor frecuencias demasiado altas.
`Modes`	Aquí se almacenan los parámetros de modeline para las resoluciones de pantalla determinadas. SaX2 calcula estos parámetros basándose en los valores introducidos por el usuario, y en general no es necesario cambiarlos. Intervenga en este punto si, por ejemplo, desea conectar un monitor de frecuencia fija. Encontrará más detalles sobre el significado de cada valor numérico en el archivo HOWTO `/usr/share/doc/howto/en/html/XFree86-Video-Timings-HOWTO`.
`Device`	Esta sección define una tarjeta gráfica determinada. Se hace referencia a la tarjeta mediante su nombre descriptivo.
`Screen`	Esta sección reune un `Monitor` y un `Device` para conformar el conjunto de ajustes necesarios para X.Org. En la subsección `Display`, especifique el tamaño de la pantalla virtual (`Virtual`), `ViewPort`, y `Modes` que se utilizarán con esta pantalla.
`ServerLayout`	Esta sección define la disposición en uno o varios monitores. En ella se relaciona los dispositivos de entrada `InputDevice` con los dispositivos de visualización `Screen`.

`Monitor`, `Device` y `Screen` se explican con más detalle a continuación. Hay más información sobre las demás secciones en las páginas Man de `X.Org` y `xorg.conf`.

Es posible encontrar varias secciones `Monitor` y `Device` diferentes en `xorg.conf`. Incluso es posible que aparezca más de una sección `Screen`. La sección `ServerLayout` que figura a continuación es la que determina qué se utilizará.

14.2.1 Sección Screen

La sección Screen combina un monitor con una sección device y determina la resolución y la profundidad del color que se debe utilizar. El aspecto de una sección Screen puede ser similar al del Ejemplo 14.1, "Sección Screen del archivo /etc/X11/xorg.conf" (p. 298).

Ejemplo 14.1 *Sección Screen del archivo /etc/X11/xorg.conf*

```
Section "Screen"
  DefaultDepth  16
  SubSection "Display"
    Depth       16
    Modes       "1152x864" "1024x768" "800x600"
    Virtual     1152x864
  EndSubSection
  SubSection "Display"
    Depth       24
    Modes       "1280x1024"
  EndSubSection
  SubSection "Display"
    Depth       32
    Modes "640x480"
  EndSubSection
  SubSection "Display"
    Depth        8
    Modes       "1280x1024"
  EndSubSection
  Device        "Device[0]"
  Identifier    "Screen[0]"
  Monitor       "Monitor[0]"
EndSection
```

La línea `Identifier` (en este ejemplo, `Screen[0]`) proporciona un nombre concreto mediante el cual se puede hacer referencia a esta sección en la sección `ServerLayout` que sigue. Las líneas `Device` y `Monitor` especifican la tarjeta gráfica y el monitor que pertenecen a esta definición. Son simples enlaces a las secciones `Device` y `Monitor` con el correspondiente nombre o *identifier*. Dichas secciones se describen en detalle a continuación.

Utilice el ajuste `DefaultDepth` para seleccionar la profundidad de color por defecto que debe utilizar el servidor si no se inicia con una específica. Existe una subsección `Display` para cada profundidad de color. La palabra clave `Depth` asigna la profundidad de color válida para cada subsección. Los valores posibles de `Depth` son 8, 15, 16 y 24. Algunos módulos del servidor X no admiten todos los valores.

Después de la profundidad de color, se define una lista de resoluciones en la sección `Modes`. El servidor X lee la lista de izquierda a derecha. Para cada resolución, el servidor X busca un `Modeline` en la sección `Modes`. La `Modeline` depende de la capacidad del monitor y de la tarjeta gráfica. Los ajustes de `Monitor` determinan la `Modeline` que se obtiene como resultado.

La primera resolución que se encuentra es la de `Default mode`. Se puede cambiar a la siguiente resolución hacia la derecha de la lista mediante Ctrl + Alt + + (del teclado numérico). Para cambiar a la siguiente resolución hacia la izquierda de la lista, use Ctrl + Alt + – (del teclado numérico). De esta manera es posible cambiar la resolución mientras se ejecuta X.

La última línea de la subsección `Display` con `Depth 16` hace referencia al tamaño de la pantalla virtual. El tamaño máximo de la pantalla virtual depende de la cantidad de memoria instalada en la tarjeta gráfica y de la profundidad de color deseada, no de la resolución máxima del monitor. Puesto que las tarjetas gráficas modernas disponen de una gran cantidad de memoria de vídeo, se pueden crear escritorios virtuales muy grandes. Sin embargo, si se ocupa mucha memoria de vídeo con un escritorio virtual, es posible que ya no se puedan aprovechar las funciones 3D. Si, por ejemplo, la tarjeta dispone de 16 MB de RAM para vídeo, la pantalla virtual puede llegar a los 4096 x 4906 píxeles de tamaño con una profundidad de color de 8 bits. Sin embargo, en especial en el caso de tarjetas con aceleración, no se recomienda utilizar toda la memoria para la pantalla virtual, ya que la memoria de la tarjeta se utiliza para diferentes cachés de fuentes y gráficos.

14.2.2 Sección Device

Cada sección device describe una tarjeta gráfica determinada. Es posible incluir en `xorg.conf` tantas entradas device como se desee, siempre que se distingan sus nombres mediante la palabra clave `Identifier`. Como norma general, si dispone de más de una tarjeta gráfica instalada, las secciones se numeran en orden. La primera se llama `Device[0]`, la segunda `Device[1]` y así sucesivamente. El siguiente archivo muestra un extracto de la sección `Device` de un equipo con una tarjeta gráfica PCI Matrox Millennium:

```
Section "Device"
  BoardName     "MGA2064W"
  BusID         "0:19:0"
  Driver        "mga"
  Identifier    "Device[0]"
  VendorName    "Matrox"
```

```
  Option        "sw_cursor"
EndSection
```

Si se utiliza SaX2 para la configuración, la sección device debería tener un aspecto similar al del ejemplo anterior. Tanto `Driver` como `BusID` dependen del hardware instalado en el equipo; SaX2 los detecta automáticamente. `BusID` define la ranura PCI o AGP en la que está instalada la tarjeta. Esto corresponde con el ID que muestra el comando lspci. El servidor X requiere que los valores estén en forma decimal, pero lspci los muestra en hexadecimal.

Mediante el parámetro `Driver`, especifique el parámetro que se utilizará para la tarjeta gráfica. Si la tarjeta es una Matrox Millennium, el módulo del controlador se llama `mga`. El servidor X buscará en la vía `ModulePath` definida en la sección `Files` del subdirectorio `drivers`. En una instalación estándar, se trata del directorio `/usr/X11R6/lib/modules/drivers`. Al nombre indicado se le añade `_drv.o`, de manera que, en el caso del controlador `mga`, se cargará el archivo `mga_drv.o`.

El comportamiento del servidor X y del controlador se puede modificar mediante opciones adicionales. Un ejemplo de ello es la opción `sw_cursor`, que se define en la sección device. Esta opción desactiva el cursor del ratón creado por hardware y lo dibuja mediante software. Hay varias opciones disponibles en función del módulo del controlador, que se pueden encontrar en los archivos de descripción de los módulos del controlador, en el directorio `/usr/X11R6/lib/X11/doc`. Las opciones válidas en general también se encuentran en las páginas Man (`man xorg.conf` y `man X.Org`).

14.2.3 Secciones Monitor y Modes

Al igual que las secciones `Device`, cada sección `Monitor` y `Modes` describe un monitor. El archivo de configuración `/etc/X11/xorg.conf` puede contener tantas secciones `Monitor` como se desee. La sección ServerLayout especifica qué sección `Monitor` es la relevante.

Las definiciones de Monitor sólo deben ser ajustadas por usuarios experimentados. Las modelines constituyen una parte importante de las secciones `Monitor`. Las modelines establecen la sincronización horizontal y vertical de la resolución respectiva. Las propiedades del monitor, en especial las frecuencias permitidas, se almacenan en la sección `Monitor`.

AVISO

No cambie ningún parámetro de las modelines a menos que tenga un conocimiento profundo del funcionamiento del monitor y de la tarjeta gráfica, ya que podrían producirse daños graves en el monitor.

Para el desarrollo de descripciones de monitor propias es necesario conocer la documentación de `/usr/X11/lib/X11/doc`. Cabe destacar el apartado dedicado a los modos de vídeo. En él se describe en detalle el funcionamiento del hardware y la manera de crear modelines.

Hoy en día la especificación manual de modelines no suele ser necesaria. Si se utiliza un monitor multifrecuencia actual, generalmente el servidor X puede obtener las frecuencias permitidas y las resoluciones óptimas directamente del monitor por medio de DDC, tal y como se describe en la sección de configuración de SaX2. Si, por cualquier razón, no fuera posible obtenerlas, utilice uno de los modos VESA que se incluyen en el servidor X. Esto funcionará con prácticamente todas las combinaciones de tarjetas gráficas y monitores.

14.3 Instalación y configuración de fuentes

La instalación de fuentes adicionales en SUSE Linux es un proceso sencillo. Sólo tiene que copiar las fuentes en cualquier directorio ubicado en la vía de fuente X11 (consulte la Sección 14.3.1, “Fuentes centrales X11” (p. 302)). Para habilitar la utilización de fuentes, el directorio de instalación debe ser un subdirectorio de los directorios configurados en `/etc/fonts/fonts.conf` (consulte la Sección 14.3.2, “Xft” (p. 303)).

Los archivos de fuentes se pueden copiar de forma manual (como `root`) en un directorio adecuado, como por ejemplo `/usr/X11R6/lib/X11/fonts/truetype`. Si no, la tarea se puede realizar mediante el instalador de fuentes KDE en el Centro de control de KDE. El resultado es el mismo.

En lugar de copiar las fuentes actuales, también puede crear enlaces simbólicos. Por ejemplo, puede realizar esto si dispone de fuentes con licencia en una partición Windows montada y desea utilizarlas. A continuación, ejecute `SuSEconfig --module fonts`.

`SuSEconfig --module fonts` ejecuta el guión `/usr/sbin/fonts-config`, que gestiona la configuración de las fuentes. Para ver lo que realiza este guión, consulte la página del manual del guión (`man fonts-config`).

El procedimiento es el mismo para fuentes de mapa de bits y fuentes TrueType, OpenType y Type1 (PostScript). Todos estos tipos de fuentes se pueden instalar en cualquier directorio. Únicamente las fuentes con clave CID requieren que se lleve a cabo un proceso ligeramente diferente. Para ello, consulte la Sección 14.3.3, “Fuentes con clave CID” (p. 306).

X.Org contiene dos sistemas de fuentes completamente diferentes: el *sistema central de fuentes X11* antiguo y el recién diseñado sistema *Xft y fontconfig*. Las secciones siguientes describen brevemente ambos sistemas.

14.3.1 Fuentes centrales X11

Hoy en día, el sistema central de fuentes X11 es compatible con fuentes de mapa de bits y también con fuentes ampliables, como Type1, TrueType y OpenType, así como fuentes con clave CID. Las fuentes ampliables sólo son compatibles sin suavización de contornos ni procesamiento de subpixeles; el inicio de fuentes ampliables grandes con glifos para varios idiomas puede tardar mucho tiempo. También se admiten fuentes Unicode, pero puede que su uso sea más lento y requiera más memoria.

El sistema central de fuentes X11 tiene algunos puntos débiles inherentes. Está obsoleto y no se puede ampliar de manera significativa. Sin embargo, debe conservarse por razones de compatibilidad retroactiva; si es posible, deben utilizarse los sistemas Xft y fontconfig que son más modernos.

Para su funcionamiento, el servidor X necesita saber las fuentes que están disponibles y la parte del sistema en la puede encontrarlas. Esto se gestiona mediante una variable FontPath, que contiene la vía de todos los directorios de fuente de sistema válidos. En cada uno de estos directorios, un archivo denominado `fonts.dir` enumera las fuentes disponibles en el directorio. El servidor X genera FontPath durante el inicio. Busca un archivo `fonts.dir` válido en cada entrada `FontPath` del archivo de configuración `/etc/X11/xorg.conf`. Estas entradas se encuentran en la sección `Files`. Muestre el FontPath actual mediante `xset q`. Esta vía se puede modificar durante el tiempo de ejecución mediante xset. Para agregar una vía adicional, utilice `xset +fp <path>`. Para eliminar una vía no deseada, utilice `xset -fp <path>`.

Si el servidor X ya está activo, las fuentes recién instaladas en los directorios montados estarán disponibles mediante el comando `xset fp rehash`. Este comando se ejecuta mediante `SuSEconfig --module fonts`. Puesto que el comando `xset` necesita acceder al servidor X en funcionamiento, esto sólo funciona si `SuSEconfig --module fonts` se inicia desde una shell que tenga acceso al servidor X en funcionamiento. La manera más fácil de llevar esto a cabo es adoptar los permisos `root` introduciendo `su` y la contraseña root. `su` transfiere los permisos de acceso del usuario que ha iniciado el servidor X al shell root. Para comprobar que las fuentes se han instalado correctamente y que están disponibles a través del sistema central de fuentes X11, utilice el comando `xlsfonts` para enumerar todas las fuentes disponibles.

Por defecto, SUSE Linux utiliza configuraciones regionales UTF-8. Por lo tanto, se preferirán fuentes Unicode (nombres de fuente que finalicen por `iso10646-1` en la salida `xlsfonts`). `xlsfonts | grep iso10646-1` enumera todas las fuentes Unicode disponibles. Aproximadamente todas las fuentes Unicode disponibles en SUSE Linux contienen por lo menos los glifos necesarios para idiomas europeos (anteriormente codificados como `iso-8859-*`).

14.3.2 Xft

Para empezar, los programadores de Xft deben asegurarse de que las fuentes ampliables con suavización de contornos sean compatibles. Si se utiliza Xft, las fuentes se procesan por la aplicación que las utilice, no por el servidor X tal y como sucedía en el sistema central de fuentes X11. De este modo, la aplicación correspondiente tiene acceso a los archivos de fuentes actuales y control completo sobre el procesamiento de los glifos. Esto constituye las bases para la correcta visualización de texto en varios idiomas. El acceso directo a los archivos de fuente resulta útil en fuentes insertadas para impresión para asegurarse de que el resultado de la impresión sea igual que el que aparece en pantalla.

En SUSE Linux, los dos entornos de escritorio KDE y GNOME, Mozilla y otras aplicaciones utilizan por defecto Xft. Ya existen más aplicaciones que utilizan Xft en lugar del antiguo sistema central de fuentes X11.

Xft utiliza la librería fontconfig para buscar fuentes e influir en su procesamiento. Las propiedades de fontconfig están controladas por el archivo de configuración global `/etc/fonts/fonts.conf` y por el archivo de configuración específico del usuario

`~/.fonts.conf`. Cada uno de estos archivos de configuración fontconfig debe comenzar por lo siguiente

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

Y finalizar por lo siguiente

```
</fontconfig>
```

Si desea agregar directorios para buscar fuentes, introduzca líneas como la siguiente:

```
<dir>/usr/local/share/fonts/</dir>
```

Sin embargo, esto no suele ser necesario. Por defecto, el directorio específico del usuario `~/.fonts` ya está incluido en `/etc/fonts/fonts.conf`. Por lo tanto, todo lo que necesita para instalar fuentes adicionales es copiarlas en `~/.fonts`.

También puede insertar reglas que afecten a la apariencia de las fuentes. Por ejemplo, introduzca

```
<match target="font"<
 <edit name="antialias" mode="assign"<
  <bool<false</bool<
 </edit<
</match<
```

para inhabilitar la suavización de contornos de todas las fuentes o

```
<match target="font">
 <test name="family">
  <string>Luxi Mono</string>
  <string>Luxi Sans</string>
 </test>
 <edit name="antialias" mode="assign">
 <bool>false</bool>
 </edit>
</match>
```

para inhabilitar la suavización de contornos de determinadas fuentes.

Por defecto, la mayoría de aplicaciones utilizan los nombres de fuente `sans-serif` (o el equivalente `sans`), `serif` o `monospace`. Estas no son fuentes reales sino alias que se traducen a una fuente adecuada en función de la configuración de idioma.

Los usuarios pueden agregar fácilmente reglas a `~/.fonts.conf` para traducir estos alias a sus fuentes favoritas:

```
<alias>
 <family>sans-serif</family>
 <prefer>
  <family>FreeSans</family>
 </prefer>
</alias>
<alias>
 <family>serif</family>
 <prefer>
  <family>FreeSerif</family>
 </prefer>
</alias>
<alias>
 <family>monospace</family>
 <prefer>
  <family>FreeMono</family>
 </prefer>
</alias>
```

Puesto que casi todas las aplicaciones utilizan estos alias por defecto, esto afecta a casi todo el sistema. Por lo tanto, puede utilizar fácilmente sus fuentes favoritas en casi todo el sistema sin necesidad de modificar la configuración de fuente de las aplicaciones individuales.

Utilice el comando `fc-list` para encontrar las fuentes instaladas y disponibles para su uso. Por ejemplo, el comando `fc-list` proporciona una lista de todas las fuentes. Para buscar en las fuentes ampliables disponibles (`:scalable=true`) las que contienen todos los glifos requeridos para hebreo (`:lang=he`), los nombres de fuente (`family`), el estilo (`style`), el tamaño (`weight`) y el nombre de los archivos que contienen las fuentes, introduzca el comando siguiente:

```
fc-list ":lang=he:scalable=true" family style weight
```

La salida de este comando aparece de la manera siguiente:

```
FreeSansBold.ttf: FreeSans:style=Bold:weight=200
FreeMonoBoldOblique.ttf: FreeMono:style=BoldOblique:weight=200
FreeSerif.ttf: FreeSerif:style=Medium:weight=80
FreeSerifBoldItalic.ttf: FreeSerif:style=BoldItalic:weight=200
FreeSansOblique.ttf: FreeSans:style=Oblique:weight=80
FreeSerifItalic.ttf: FreeSerif:style=Italic:weight=80
FreeMonoOblique.ttf: FreeMono:style=Oblique:weight=80
FreeMono.ttf: FreeMono:style=Medium:weight=80
FreeSans.ttf: FreeSans:style=Medium:weight=80
FreeSerifBold.ttf: FreeSerif:style=Bold:weight=200
FreeSansBoldOblique.ttf: FreeSans:style=BoldOblique:weight=200
FreeMonoBold.ttf: FreeMono:style=Bold:weight=200
```

Parámetros importantes que se pueden consultar con `fc-list`:

Tabla 14.2 *Parámetros de fc-list*

Parámetro	Significado y valores posibles
`family`	Nombre de la familia de la fuente, por ejemplo, `FreeSans`.
`foundry`	Fabricante de la fuente, por ejemplo, `urw`.
`style`	Estilo de la fuente, como por ejemplo `Medium`, `Regular`, `Bold`, `Italic` o `Heavy`.
`lang`	Idioma compatible con la fuente, por ejemplo, `de` para alemán, `ja` para japonés, `zh-TW` para chino tradicional o `zh-CN` para chino simplificado.
`weight`	Tamaño de la fuente, como por ejemplo `80` para letra redonda o `200` para negrita.
`slant`	Inclinación, generalmente `0` para ninguna inclinación y `100` para cursiva.
`file`	Nombre del archivo que contiene la fuente.
`outline`	`true` para fuentes con contorno o `false` para el resto.
`scalable`	`true` para fuentes ampliables o `false` para el resto.
`bitmap`	`true` para fuentes de mapas de bits o `false` para el resto.
`pixelsize`	Tamaño de la fuente en píxeles. En una conexión con fc-list, esta opción sólo es útil para fuentes de mapa de bits.

14.3.3 Fuentes con clave CID

A diferencia de otros tipos de fuentes, no puede instalar simplemente fuentes con clave CID en cualquier directorio. Las fuentes con clave CID deben instalarse en `/usr/`

`share/ghostscript/Resource/CIDFont`. Esto no es relevante para Xft y fontconfig, pero es necesario para Ghostscript y para el sistema central de fuentes X11.

SUGERENCIA

Consulte `http://www.xfree86.org/current/fonts.html` para obtener más información acerca de las fuentes que se ejecutan en X11.

14.4 OpenGL: configuración 3D

14.4.1 Compatibilidad de hardware

SUSE Linux incluye varios controladores de OpenGL para ofrecer compatibilidad con el hardware 3D. En la Tabla 14.3, “Hardware 3D compatible” (p. 307) se ofrece un resumen.

Tabla 14.3 *Hardware 3D compatible*

Controlador de OpenGL	Hardware compatible
nVidia	Tarjetas nVidia: todas excepto algunos chipsets heredados (GeForce2 y anteriores)
DRI	Intel i810/i815/i830M,
	Intel 845G/852GM/855GM/865G/915G,915GM/945G
	Matrox G200/G400/G450/G550,
	ATI Rage 128(Pro)/Radeon (hasta el modelo 9250)

Si está instalando mediante YaST por primera vez, puede activar la aceleración 3D durante la instalación, ya que YaST detecta la compatibilidad 3D. Para las tarjetas gráficas nVidia, se debe instala primero el controlador de nVidia. Para ello, seleccione el parche del controlador de nVidia en YOU (YaST Online Update). Debido a las restricciones de la licencia, el controlador de nVidia no se incluye en la distribución.

Si en su lugar, está actualizando el sistema, el procedimiento para configurar la compatibilidad con el hardware 3D es distinta: dependerá del controlador de OpenGL que se utilice. En la siguiente sección se ofrecen más detalles.

14.4.2 Controladores de OpenGL

Los controladores de OpenGL nVidia y DRI se pueden configurar fácilmente mediante SaX2. Para los adaptadores nVidia, se debe instalar primero el controlador de nVidia. Escriba el comando `3Ddiag` para comprobar si la configuración para nVidia o DRI es correcta.

Por motivos de seguridad, sólo los usuarios que pertenezcan al grupo `video` tendrán permiso para acceder al hardware 3D. Por lo tanto, asegúrese de que todos los usuarios locales sean miembros de este grupo. De otra forma, se utilizaría el lento *software de análisis de respaldo* del controlador de OpenGL para las aplicaciones OpenGL. Utilice el comando `id` para comprobar si el usuario actual pertenece al grupo `video`. Si no es así, utilice YaST para añadirlo.

14.4.3 Herramienta de diagnóstico 3Ddiag

La herramienta de diagnóstico 3Ddiag permite verificar la configuración 3D de SUSE Linux. Se trata de una herramienta de línea de comandos que se debe abrir en un terminal. Escriba `3Ddiag -h` para mostrar una lista de las opciones que 3Ddiag admite.

Para verificar la configuración de X.Org, la herramienta comprueba si los paquetes necesarios para la compatibilidad 3D están instalados y si se usan la biblioteca OpenGL y la extensión GLX correctas. Siga las instrucciones de 3Ddiag si recibe mensajes de error. Si todo está correcto, sólo verá en la pantalla los mensajes de tareas finalizadas.

14.4.4 Utilidades de prueba de OpenGL

Para probar OpenGL, pueden resultar de utilidad el programa `glxgears` y juegos como `tuxracer` o `armagetron` (sus paquetes tienen los mismos nombres). Si se ha activado la compatibilidad 3D, debería ser posible ejecutarlos sin problemas en un equipo nuevo. Sin la compatibilidad 3D, estos juegos se ejecutarían muy lentamente (efecto de proyección de diapositivas). Utilice el comando `glxinfo` para comprobar

si la compatibilidad 3D está activada, en cuyo caso, el resultado contendrá la línea `direct rendering: Yes`.

14.4.5 Solución de problemas

Si los resultados de la prueba 3D de OpenGL son negativos (los juegos no funcionan con soltura), utilice 3Ddiag para asegurarse de que no existen errores en la configuración (mensajes de error). Si tras corregirlos no se soluciona el problema, o si no han aparecido mensajes de error, estudie los archivos de registro de X.Org.

A menudo encontrará la línea `DRI is disabled` en el archivo `/var/log/Xorg.0.log` de X.Org. La causa exacta sólo se puede determinar examinando detalladamente el archivo de registro, una tarea que requiere cierta experiencia.

En estos casos, no existe ningún error de configuración, ya que 3Ddiag los habría detectado. Por lo tanto, en este punto, la única opción es utilizar el software de análisis de respaldo del controlador de DRI, que no ofrece compatibilidad para hardware 3D. También tendrá que continuar sin compatibilidad 3D si se presentan errores de representación de OpenGL o si el sistema se vuelve inestable. Utilice SaX2 para deshabilitar totalmente la compatibilidad 3D.

14.4.6 Asistencia para la instalación

Aparte del `software de análisis de respaldo` del controlador de DRI, algunos controladores de OpenGL de Linux siguen estando en fase de desarrollo y, por lo tanto, se consideran experimentales. Los controladores se incluyen en la distribución por la alta demanda de aceleración 3D de hardware existente entre los usuarios de Linux. Teniendo en cuenta el estado experimental de algunos controladores de OpenGL, SUSE no puede ofrecer asistencia alguna de instalación para configurar la aceleración 3D por hardware ni asistencia posterior sobre problemas relacionados. La configuración básica de la interfaz gráfica del usuario (sistema X Window) no incluye la configuración de la aceleración 3D por hardware. Si experimenta problemas con este tipo de aceleración, se recomienda deshabilitar totalmente la compatibilidad 3D.

14.4.7 Información adicional

Para obtener más información, consulte los archivos README (Léame) de `/usr/X11R6/lib/X11/doc`. Encontrará más información sobre la instalación del controlador de nVidia en `http://www.suse.de/~sndirsch/nvidia-installer-HOWTO.html`.

FreeNX: control remoto de otro equipo

15

FreeNX es una implementación GPL del servidor NX, que se utiliza para acceder de forma remota y mostrar otro equipo. Ofrece una velocidad de respuesta de las aplicaciones cercana a la del funcionamiento local mediante enlaces de banda estrecha de alta latencia.

15.1 Procedimientos iniciales de NX

En los siguientes pasos se describen los procedimientos básicos para establecer una instalación de trabajo de NX que permita que hasta 10 clientes se conecten al servidor NX.

1 Instale los siguientes paquetes en los equipos servidor y cliente mediante el módulo de gestión de software de YaST:

Equipo servidor	Equipo cliente
• `NX` • `FreeNX`	• `NX` • `knx` (para sesiones de KDE) • NoMachine `nxclient` (para sesiones distintas a KDE)

2 Instale el servidor NX emitiendo el siguiente comando como usuario Root:

```
nxsetup --install --clean --purge --setup-nomachine-key
```

El servidor se abrirá y se ejecutará según los ajustes por defecto de `/etc/nxserver/node.conf`. Cualquier usuario podrá conectarse de forma remota desde otra estación de trabajo. Para obtener información sobre la configuración avanzada del servidor NX, consulte la Sección 15.2, “Configuración avanzada de FreeNX” (p. 314).

Si prefiere realizar una instalación más segura con claves privadas distribuidas a cada cliente, consulte las instrucciones descritas en la Sección 15.2.1, “Configuración de la autenticación SSH mediante claves de cliente” (p. 314).

3 Configure el cortafuegos en el equipo que albergue el servidor NX para permitir las conexiones NX.

a Inicie sesión en el equipo servidor como usuario Root y abra el modulo de cortafuegos de YaST.

b Seleccione *Servicios autorizados* para acceder al cuadro de diálogo de configuración de servicios y haga clic en *Zona externa.*

c Haga clic en *Avanzado* para indicar los detalles del puerto para NX.

d Abra los puertos 22 (SSH), 5000 a 5009 y 7000 a 7009 para permitir el tráfico de NX. Puede hacerlo escribiendo lo siguiente en *Puertos TCP:*

```
22 5000:5009 7000:7009
```

e Guarde sus ajustes y reinicie el cortafuegos haciendo clic en *Aceptar* → *Siguiente* → *Aceptar.*

SUGERENCIA

Para obtener información detallada sobre la configuración del cortafuegos para NX, consulte el archivo `/usr/share/doc/packages/FreeNX/NX-Firewall.txt`.

Para conectarse de forma remota a otra estación de trabajo y utilizar KDE como escritorio, siga este procedimiento:

1. Inicie KNX desde el menú principal.

2. La primera vez que inicie sesión tendrá que crear una conexión nueva. Para crear una conexión, realice el procedimiento siguiente:

   a. En *KNX Client Login* (Inicio de sesión de cliente de KNX), haga clic en *Connection Settings* (Configuración de la conexión).

   b. Indique un nombre para la conexión, por ejemplo, el nombre del servidor.

   c. Indique la información del host, el número del puerto y el ancho de banda de la conexión.

   d. En *Session type* (Tipo de sesión), seleccione *UNIX/KDE* para abrir una sesión de KDE.

   e. Seleccione una resolución de pantalla.

   f. Haga clic en *Aceptar*.

3. Cuando esté conectado y aparezca la conexión remota en la pantalla, podrá acceder a las aplicaciones y utilizar el equipo remoto como si estuviera frente a ese equipo.

Para conectarse de forma remota a otro equipo utilizando GNOME como escritorio, siga este procedimiento:

1. Descargue e instale el paquete nxclient de NoMachine mediante `http://www.nomachine.com/download_client_linux.php`.

2. Abra el asistente para la conexión de NX desde el menú principal.

3. En tres pasos, indique el nombre de la conexión, el puerto y los detalles del host y el tipo de conexión; seleccione el tipo de sesión *Unix/Gnome,* decida si desea crear un acceso directo en el escritorio y, por último, haga clic en *Finalizar.*

4. Para conectarse al escritorio remoto, haga clic en el acceso directo de NX del escritorio, indique el nombre de usuario y la contraseña y haga clic en *Aceptar.*

   El escritorio remoto aparecerá en la pantalla.

15.2 Configuración avanzada de FreeNX

En las siguientes secciones se presentan algunas funciones avanzadas, necesarias sobre todo en escenarios de NX más complejos.

15.2.1 Configuración de la autenticación SSH mediante claves de cliente

La autenticación configurada en la Sección 15.1, “Procedimientos iniciales de NX” (p. 311) se basa únicamente en un nombre de usuario y una contraseña. Para conseguir un sistema de autenticación más seguro, es posible configurar NX para que genere un par de claves SSH. La clave de cliente se copia entonces desde el equipo servidor en cualquier cliente que deba conectarse al servidor NX. Los clientes que no cuenten con esta clave no podrán autenticarse en el servidor NX. Esta función sólo se admite para la combinación servidor FreeNX/cliente KNX.

Para configurar el servidor NX para que utilice este método de autenticación y genere el par de claves adecuado, siga este procedimiento:

1. Inicie sesión como usuario Root en el equipo servidor.
2. Abra el archivo de configuración del servidor `/etc/nxserver/node.conf` y asegúrese de que la variable `ENABLE_SSH_AUTHENTICATION` está definida en `1` (que es el valor por defecto).
3. Instale el servidor con el siguiente comando:

   ```
   nxsetup --install --clean --purge
   ```

4. Ajuste los permisos de acceso en `/var/lib/nxserver/home/.ssh/authorized_keys2`:

   ```
   chmod 640 /var/lib/nxserver/home/.ssh/authorized_keys2
   ```

5. Cierre la sesión.

Para configurar KNX a fin de que utilice esta clave, siga este procedimiento:

1. En el equipo servidor, inicie sesión como usuario Root.

2. Copie el archivo de clave a la ubicación del equipo cliente que solicite KNX, y sustituya *cliente* por la dirección del cliente.

   ```
   scp /var/lib/nxserver/home/.ssh/client.id_dsa.key cliente/usr/share/knx/
   ```

3. Inicie sesión como usuario Root en el equipo cliente.

4. Ajuste los permisos de acceso así:

   ```
   chmod 644 /usr/share/knx/client.id_dsa.key
   ```

5. Cierre la sesión.

15.2.2 Configuración de la autenticación PAM.

Por defecto, FreeNX permite que cualquier usuario abra una sesión de NX, siempre que tal usuario esté presente en la base de datos de usuarios del servidor (de forma local o mediante LDAP, NIS, etc.). Este comportamiento lo regula la variable `ENABLE_PAM_AUTHENTICATION` del archivo `/usr/bin/nxserver` del equipo servidor. El valor por defecto es `1`. Si se establece en `0`, se deshabilitará la autenticación de usuarios mediante PAM (`PAM_AUTH`) en FreeNX.

Si `ENABLE_PAM_AUTHENTICATION` se define como `0`, tendrá que añadir los usuarios y sus contraseñas de forma manual. Para añadir usuarios de NX locales en el servidor, siga este procedimiento:

1. Inicie sesión como usuario Root en el equipo servidor.

2. Asegúrese de que cualquier usuario que añada esté presente en la base de datos de usuarios locales del sistema. Para ello compruebe el contenido de `/etc/passwd` o utilice el módulo de gestión de usuarios de YaST.

3 Añada el nombre de usuario de cada usuario que desee añadir mediante el comando `nxserver --adduser`. A continuación, añada sus contraseñas mediante `nxserver --passwd`.

4 Reinicie el servidor con `nxserver --restart` y salga de la sesión.

15.2.3 Uso de archivos de configuración para usuarios concretos o para todo el sistema

El comportamiento del servidor FreeNX se controla mediante el archivo `/etc/node.conf`. Es posible aplicar una configuración de servidor NX global o configuraciones específicas para cada usuario. Esta última forma se puede aplicar si hay varios usuarios de NX en un equipo que tienen distintas necesidades.

En el ejemplo siguiente, imagine que el usuario `juan` desea que NX se inicie automáticamente con una aplicación determinada en cuanto se abra una sesión de NX. Para permitir esta acción sólo para este usuario, siga este procedimiento:

1 Inicie sesión como usuario Root.

2 Entre en el directorio `/etc/nxserver`.

```
cd /etc/nxserver
```

3 Guarde una copia del archivo de configuración del servidor NX (`node.conf`), situado bajo `juan.node.conf` en el mismo directorio.

4 Modifique los parámetros oportunos (`NODE_AUTOSTART` y `ENABLE_AUTORECONNECT`) en `juan.node.conf`. Para obtener más información sobre estas funciones, consulte la Sección 15.2.5, “Configuración de las tareas de inicio automático y ajustes de exportación” (p. 317) y la Sección 15.2.4, “Suspensión y reanudación de sesiones de NX” (p. 317).

5 Vuelva a instalar el servidor NX para activar la nueva configuración:

```
nxsetup --install --clean --purge --setup-nomachine-key
```

La configuración específica para el usuario sustituirá a la configuración global.

6 Cierre la sesión.

15.2.4 Suspensión y reanudación de sesiones de NX

Al igual que ocurre con las sesiones de los equipos portátiles, es posible configurar NX para que permita la suspensión y reanudación de sesiones de usuarios. Cuando se reabre, la sesión suspendida vuelve a estar exactamente en el mismo estado en el que se dejó.

Para configurar la suspensión y reanudación de sesiones de NX, siga este procedimiento:

1 Inicie sesión como usuario Root.

2 Abra el archivo de configuración del servidor, `/etc/nxserver/node.conf`, y modifíquelo así:

```
ENABLE_PASSDB_AUTHENTICATION="0"
ENABLE_USER_DB="0"
ENABLE_AUTORECONNECT="1"
```

3 Guarde y salga del archivo de configuración y reinicie el servidor mediante el comando `nxserver --restart`.

4 Cierre la sesión.

Para suspender una sesión al salir, haga clic en la *X* de la esquina superior derecha de la ventana de NX y seleccione *Suspender* para suspender la sesión y salir del cliente. Cuando vuelva a conectar se le preguntará si desea reanudar la sesión anterior o iniciar una nueva.

15.2.5 Configuración de las tareas de inicio automático y ajustes de exportación

FreeNX ofrece una función de inicio automático que permite abrir algunas tareas al iniciar o reanudar una sesión de NX, siempre que la aplicación subyacente admita las propiedades `start` y `resume`. Por ejemplo, se puede limpiar automáticamente el escritorio o realizar otras tareas automáticas al iniciar FreeNX. Esta función es muy

útil al reconectar una sesión, incluso desde un cliente de NX distinto (desde el que no se puedan utilizar los mecanismos de KDE o GNOME estándar).

Para configurar las funciones de inicio automático, siga este procedimiento:

1. Inicie sesión como usuario Root en el equipo servidor.

2. Abra el archivo de configuración del servidor `/etc/nxserver/node.conf` y modifique la variable `NODE_AUTOSTART` de la siguiente forma, sustituyendo *`miprograma`* por el programa que se deba ejecutar al iniciar o reanudar una sesión de NX:

   ```
   NODE_AUTOSTART=miprograma
   ```

3. Guarde y salga del archivo de configuración.

4. Reinicie el servidor con el comando `nxserver --restart` y salga de la sesión.

   El programa indicado se abrirá cada vez que se inicie o reanude una sesión.

También se pueden exportar las variables `NX_USERIP` y `NX_SESSIONID` para que los demás usuarios del entorno puedan acceder a ellas. De esta forma será posible, por ejemplo, colocar un icono en el escritorio con el contenido genérico y acceder al servidor Samba que se ejecute en el cliente de procesamiento parcial del usuario. Para hacer que el contenido de un disquete de la unidad de disquetes del cliente de procesamiento parcial esté a disposición del usuario, siga este procedimiento:

1. Habilite la exportación de las variables `NX_USERIP` y `NX_SESSIONID` en el servidor:

   a. Inicie sesión como usuario Root en el equipo servidor.

   b. Abra el archivo de configuración del servidor, `/etc/nxserver/node.conf`, y defina las siguientes variables:

      ```
      EXPORT_USERIP="1"
      EXPORT_SESSIONID="1"
      ```

   c. Guarde y salga del archivo de configuración y reinicie el servidor mediante el comando `nxserver --restart`.

d Cierre la sesión.

2 En el cliente, abra una sesión, exporte la unidad de disquete mediante SMB y cree un icono en el escritorio:

a Exporte el contenido de la unidad de disquete mediante Samba utilizando su gestor de archivos (Nautilus o Konqueror).

b Cree un archivo `floppy.desktop` en el directorio `Desktop` y escriba la siguiente línea:

```
Exec=smb://$NX_USERIP/floppy
```

El servidor exportará la dirección IP del cliente de procesamiento parcial, permitiendo el acceso a la unidad de disquete de este cliente a través del icono de disquete de la sesión de NX.

15.2.6 Creación de una cadena de servidores NX

Una cadena de servidores NX permite atravesar cortafuegos y enfrentarse al enmascaramiento de IP. Se puede utilizar un servidor "gateway" externo para remitir las conexiones entrantes a un servidor interno oculto (enmascarado) tras un cortafuegos.

Para configurar una cadena de servidores NX, siga este procedimiento:

1 Configure el servidor interno tal y como se describe en la Sección 15.2.1, "Configuración de la autenticación SSH mediante claves de cliente" (p. 314) y distribuya la clave privada del servidor (`client.id_dsa.key`) a `/usr/NX/share/` en el gateway.

2 En el servidor gateway, haga lo siguiente:

a Inicie sesión como usuario Root.

b Defina las siguientes variables de `/etc/nxserver/node.conf`, sustituyendo *`mihostinterno`* por la dirección IP del servidor NX interno:

```
ENABLE_SERVER_FORWARD="1"
SERVER_FORWARD_HOST="mihostinterno"
SERVER_FORWARD_KEY="/usr/NX/share/client.id_dsa.key"
```

c Reinicie el servidor externo para aplicar la configuración modificada con el comando `nxserver --restart` y salga de la sesión.

Todas las conexiones entrantes se remitirán al servidor interno.

15.2.7 Instalación y ejecución de FreeNX y NoMachine en el mismo servidor

Es posible instalar y ejecutar FreeNX y el servidor comercial NoMachine NX en el mismo equipo sin que se produzcan interferencias. Esta función se implementa en FreeNX remitiendo la conexión al servidor NoMachine instalado en el mismo equipo.

Para habilitar esta función, siga este procedimiento:

1. Inicie sesión como usuario Root en el equipo servidor.
2. Abra el archivo de configuración del servidor para FreeNX de `/etc/nxserver/node.conf` y defina la siguiente variable:

   ```
   ENABLE_NOMACHINE_FORWARD="1"
   ```

3. Guarde este archivo y reinicie el servidor FreeNX mediante el comando `nserver --restart`.
4. Cierre la sesión.

Para conectarse al servidor NoMachine, utilice su nombre de usuario y contraseña habituales. Para conectarse al servidor FreeNX, añada el prefijo `freenx.` al nombre de usuario habitual (por ejemplo, `freenx.juangarcia`) y utilice la contraseña habitual.

15.3 Solución de problemas

En las siguientes secciones se mencionan algunos de los problemas más frecuentes que se pueden presentar al utilizar FreeNX y se ofrecen posibles soluciones.

15.3.1 KNX se bloquea al intentar establecer una conexión

Está intentando establecer una conexión con el servidor NX mediante KNX. Al iniciar la conexión, KNX es incapaz de autenticar al usuario y la sesión remota no se inicia.

Para determinar la causa de este error y averiguar cómo solucionarlo, siga este procedimiento:

1. Compruebe si Novell AppArmor se está ejecutando en el servidor y proceda como se describe en la Sección 15.3.2, “No se puede establecer la conexión con el servidor NX” (p. 322).

2. Vuelva a intentar el establecimiento de la conexión entre KNX y el servidor.

3. Compruebe si el cortafuegos del cliente permite el tráfico SSH. Para ello, abra el módulo de cortafuegos de YaST y compruebe si SSH aparece en la lista *Servicios autorizados* de la *Zona externa.* Habilite SSH si no está ya habilitado.

4. Compruebe si se permiten las conexiones SSH en el cortafuegos del servidor para los puertos de NX indicados en la Sección 15.1, “Procedimientos iniciales de NX” (p. 311). Abra estos puertos si están cerrados.

5. Vuelva a intentar el establecimiento de la conexión entre KNX y el servidor.

6. Inicie sesión como usuario Root en el servidor y siga este procedimiento:

   a. Entre en el directorio `/tmp` y busque archivos bloqueados del servidor NX:

   ```
   cd /
   ls -ltr .nX*
   ```

   b. Si hay alguno de estos archivos bloqueados antiguos, bórrelos.

c Cierre la sesión.

7 Vuelva a intentar el establecimiento de la conexión entre KNX y el servidor.

8 En el equipo cliente, desinstale y vuelva a instalar el cliente KNX mediante el módulo de gestión de software de YaST.

Tras seguir todas las instrucciones anteriores, debería ser capaz de conectarse al servidor.

15.3.2 No se puede establecer la conexión con el servidor NX

Tras abrir KNX e iniciar la conexión, obtiene el siguiente mensaje de error:

```
Connection to NX server could not be established. (No se puede establecer la
 conexión con el servidor NX.) Connection timed out. (Tiempo de espera de
conexión agotado.)
```

Para determinar el origen de este problema, siga este procedimiento:

1 Inicie sesión como usuario Root en el equipo servidor.

2 Busque en el resultado del comando `dmesg` una entrada como la siguiente:

```
SubDomain: REJECTING r access to
/var/lib/nxserver/home/.ssh/authorized_keys2 (sshd(31247) profile
/usr/sbin/sshd active /usr/sbin/sshd)
```

Esta entrada indica que Novell AppArmor, que se está ejecutando en el servidor, no permite al daemon ssh acceder a algunos archivos específicos de NX.

3 Detenga AppArmor en el equipo servidor.

O bien

Ponga el perfil de sshd en modo de aprendizaje y añada permisos para acceder a los archivos de NX en el perfil existente. Este procedimiento se describe en más detalle en la *Guía de administración de Novell AppArmor 2.0*.

4 Vuelva a conectar con el servidor.

15.3.3 La autenticación de usuario se efectúa correctamente, pero la conexión remota no se establece

Tras abrir KNX e iniciar la sesión, KNX autentica correctamente al usuario, pero en lugar de una ventana de terminal con una nueva sesión, se obtiene un mensaje de error como el siguiente:

```
Could not yet establish the connection to the remote proxy. (No es posible
establecer la conexión con el alterno remoto.) Do you want to terminate the
current session? (¿Desea finalizar la sesión actual?)
```

La conexión ha fallado debido a que los puertos superiores que se utilizan para negociar la sesión remota de NX no se han abierto en el cortafuegos del servidor. Para ajustar el cortafuegos del servidor, siga el procedimiento descrito en la Sección 15.1, “Procedimientos iniciales de NX” (p. 311).

15.4 Información adicional

Para obtener la información más reciente sobre el paquete actual de FreeNX, consulte el archivo README (Léame) `/usr/share/doc/packages/FreeNX/README.SUSE`. Para obtener información adicional acerca del servidor NX, utilice el comando `nxserver --help`.

16 Autenticación con PAM

Linux utiliza PAM (Pluggable Authentication Modules, Módulos de autenticación conectables) en el proceso de autenticación como una capa que media entre el usuario y la aplicación. Los módulos PAM están disponibles para todo el sistema, por lo que los puede solicitar cualquier aplicación. Este capítulo describe cómo funciona el mecanismo de autenticación modular y cómo se configura.

Los administradores de sistemas y los programadores suelen restringir el acceso a ciertas partes del sistema o limitar el uso de ciertas funciones de una aplicación. Sin PAM, sería necesario adaptar las aplicaciones cada vez que se introdujera un nuevo mecanismo de autenticación, como LDAP o SAMBA. Sin embargo, este proceso lleva bastante tiempo y tiende a producir errores. Una manera de evitar estos inconvenientes es separar las aplicaciones del mecanismo de autenticación y delegarlas en módulos gestionados centralmente. Cuando sea necesario utilizar un nuevo esquema de autenticación, bastará con adaptar o escribir un módulo PAM adecuado para que el programa en cuestión pueda utilizarlo.

Todos los programas que se sirven del mecanismo PAM tienen su propio archivo de configuración en el directorio `/etc/pam.d/`*`nombreprograma`*. Estos archivos definen los módulos PAM empleados en el proceso de autenticación. Además, existen archivos de configuración globales para la mayoría de los módulos PAM en `/etc/security`, los cuales definen el comportamiento exacto de estos módulos (por ejemplo `pam_env.conf`, `pam_pwcheck.conf`, `pam_unix2.conf` y `time.conf`). Todas las aplicaciones que utilicen un módulo PAM llamarán a un conjunto de funciones PAM, las cuales procesarán después la información en los distintos archivos de configuración y devolverán el resultado a la aplicación que ha realizado la llamada.

16.1 Estructura de archivos de configuración PAM

Cada línea dentro de un archivo de configuración PAM contiene un máximo de cuatro columnas:

```
<Tipo de módulo> <Indicador de control> <Vía al módulo> <Opciones>
```

Los módulos PAM se procesan en stacks. Los distintos tipos de módulos sirven a propósitos distintos, por ejemplo, un módulo comprueba la contraseña, otro verifica la ubicación desde la que se accede al sistema y otro lee los ajustes específicos del usuario. PAM reconoce cuatro tipos de módulos diferentes:

`auth`
: El objetivo de este tipo de módulo es comprobar la autenticidad del usuario. Esto se hace tradicionalmente solicitando una contraseña, si bien también se puede conseguir con la ayuda de una tarjeta de chip o mediante biométrica (huellas digitales o exploración de retina).

`cuenta`
: Los módulos de este tipo comprueban que el usuario tenga permiso general para utilizar el servicio solicitado. Por ejemplo, deberá realizarse esta comprobación para garantizar que nadie inicie sesión con el nombre de usuario de una cuenta caducada.

`password`
: El propósito de este tipo de módulo es permitir modificar un testigo de autenticación. En la mayoría de los casos, se trata de una contraseña.

`sesión`
: Los módulos de este tipo son responsables de gestionar y configurar sesiones de usuario. Estos módulos se inician antes y después de la autenticación para registrar intentos de inicio de sesión en los registros del sistema y para configurar el entorno específico del usuario (cuentas de correo, directorio personal, límites del sistema, etc.).

La segunda columna contiene indicadores de control para influir en el comportamiento de los módulos iniciados:

`required`
: Los módulos con este indicador se deben procesar correctamente antes de proceder con la autenticación. Si falla un módulo con el indicador `required`, se procesará el resto de módulos de este tipo antes de que el usuario reciba un aviso de que se ha producido un fallo durante el intento de autenticación.

`requisite`
: Los módulos con este indicador tienen que ser procesados correctamente, igual que los módulos con el indicador `required`. No obstante, si se produce un fallo en un módulo con este indicador, el usuario recibirá una notificación inmediata y no se procesarán más módulos. En caso de que no haya errores, se seguirá procesando el resto de los módulos, al igual que en el caso de los módulos con el indicador `required`. El indicador `requisite` se puede utilizar como un filtro simple con el objeto de comprobar el cumplimiento de determinadas condiciones necesarias para una correcta autenticación.

`sufficient`
: Si se procesa correctamente un modulo con este indicador, la aplicación que lo ha iniciado recibe inmediatamente una notificación de proceso correcto y no se procesa ningún otro módulo, siempre y cuando anteriormente no haya fallado la ejecución de ningún módulo con el indicador `required`. El fallo de un módulo con indicador `sufficient` no tiene consecuencias directas y los módulos siguientes se seguirán procesando según el orden correspondiente.

`optional`
: Que el proceso de un módulo con este indicador se lleve a cabo correctamente o haya errores no tiene consecuencias directas. Esta opción puede ser útil, por ejemplo, para módulos cuyo único cometido es mostrar un mensaje (por ejemplo informando al usuario acerca de la recepción de un mensaje de correo electrónico), sin realizar ninguna otra acción.

include
: Si se da este indicador, el archivo especificado como argumento se inserta en este lugar.

La vía al módulo no tiene por qué especificarse de forma explícita siempre que el módulo se encuentre en el directorio por defecto `/lib/security` (en todas las plataformas de 64 bits compatibles con SUSE Linux, el directorio es `/lib64/security`). La cuarta columna puede contener una opción para el módulo, como `debug` (activa la depuración) o `nullok` (permite utilizar contraseñas vacías).

16.2 Configuración PAM para sshd

Tomemos la configuración PAM para sshd para demostrar la teoría con un ejemplo práctico de funcionamiento:

Ejemplo 16.1 *Configuración PAM para sshd*

```
#%PAM-1.0
auth     include        common-auth
auth     required       pam_nologin.so
account  include        common-account
password include        common-password
session  include        common-session
# Habilite la siguiente línea para obtener compatibilidad de resmgr con
# sesiones ssh (consulte /usr/share/doc/packages/resmgr/README.SuSE)
#sesión opcional      pam_resmgr.so nombretty_simulado
```

La configuración típica PAM de una aplicación (sshd en este caso) contiene instrucciones que hacen referencia a los archivos de configuración de cuatro tipos de módulos: `common-auth`, `common-account`, `common-password` y `common-session`. Estos cuatro archivos contienen la configuración predeterminada para cada tipo de módulo. Si se incluyen estos archivos en lugar de llamar a cada módulo por separado para cada aplicación PAM, se obtendrá automáticamente una configuración PAM actualizada cuando el administrador cambie los ajustes por defecto. Antiguamente, era necesario ajustar todos los archivos de configuración manualmente en todas las aplicaciones cuando se producían cambios en PAM o cuando se instalaba una aplicación nueva. Ahora, la configuración PAM se lleva a cabo mediante archivos de configuración centrales y todos los cambios se heredan automáticamente en la configuración PAM de cada servicio.

El primer archivo incluido (`common-auth`) llama a dos módulos del tipo `auth`: `pam_env` y `pam_unix2`. Consulte el Ejemplo 16.2, “Configuración por defecto de la sección `auth`” (p. 328).

Ejemplo 16.2 *Configuración por defecto de la sección auth*

```
auth    required        pam_env.so
auth    required        pam_unix2.so
```

El primero, `pam_env`, carga el archivo `/etc/security/pam_env.conf` para definir las variables de entorno tal y como se especifique en este archivo. Esto se puede utilizar para definir la variable `DISPLAY` con el valor adecuado, ya que el módulo `pam_env` conoce la ubicación desde la cual se está iniciando sesión. El segundo, `pam`

_unix2, comprueba el inicio de sesión del usuario y su contraseña comparándolos con /etc/passwd y /etc/shadow.

Una vez iniciados correctamente los módulos especificados en common-auth, un tercer módulo llamado pam_nologin comprueba si existe el archivo /etc/nologin. Si existe, sólo podrá iniciar sesión el usuario Root. El stack entero de módulos auth se procesará antes de que sshd obtenga información alguna acerca de si se ha podido iniciar correctamente la sesión. Dado que todos los módulos del stack tienen el indicador de control required, deberán procesarse correctamente todos para que sshd reciba un mensaje notificándole que el resultado ha sido correcto. Aunque alguno de los módulos no llegase a procesarse correctamente, el resto del stack de módulos sí continuaría procesándose y, sólo entonces, sshd recibiría notificación acerca del resultado incorrecto.

Si se procesan correctamente todos los módulos del tipo auth, se procesará otra declaración de inclusión, en este caso, la que aparece en el Ejemplo 16.3, "Configuración por defecto de la sección account" (p. 329). common-account contiene sólo un módulo, pam_unix2. Si pam_unix2 indica como resultado que el usuario existe, sshd recibe un mensaje de notificación al respecto y se pasa a procesar el siguiente stack de módulos (password), los cuales se describen en el Ejemplo 16.4, "Configuración por defecto de la sección password" (p. 329).

Ejemplo 16.3 *Configuración por defecto de la sección account*

```
account required        pam_unix2.so
```

Ejemplo 16.4 *Configuración por defecto de la sección password*

```
password required       pam_pwcheck.so  nullok
password required       pam_unix2.so    nullok use_first_pass use_authtok
#contraseña necesaria      pam_make.so     /var/yp
```

De nuevo, la configuración PAM de sshd lleva sólo una declaración de inclusión que hace referencia a la configuración por defecto de los módulos password del archivo common-password. Estos módulos deben completarse correctamente (indicador de control required) siempre que la aplicación solicite que se cambie un testigo de autenticación. Cambiar una contraseña u otro testigo de autenticación exige realizar una comprobación de seguridad. Ésta la lleva a cabo el módulo pam_pwcheck. El módulo pam_unix2 que se utiliza posteriormente lleva consigo todas las contraseñas antiguas y nuevas de pam_pwcheck para que el usuario no tenga que volver a autenticarlas. Esto también evita que se puedan saltar las comprobaciones que lleva a cabo pam_pwcheck. Los módulos del tipo password deben utilizarse siempre que los

módulos precedentes del tipo `account` o `auth` estén configurados para emitir quejas en caso de que las contraseñas hayan caducado.

Ejemplo 16.5 *Configuración por defecto de la sección session*

```
session required        pam_limits.so
session required        pam_unix2.so
```

En el último paso, se ordena a los módulos del tipo `session`, incluidos en el archivo `common-session` que configuren la sesión según los ajustes del usuario en cuestión. Si bien `pam_unix2` se vuelve a procesar, no tiene consecuencias prácticas debido a su opción `none`, especificada en el correspondiente archivo de configuración de este módulo, `pam_unix2.conf`. El módulo `pam_limits` carga el archivo `/etc/security/limits.conf`, el cual puede definir los límites de uso de ciertos recursos del sistema. Cuando el usuario termina la sesión, se vuelve a llamar a los módulos `session`.

16.3 Configuración de módulos PAM

Algunos de los módulos PAM se pueden configurar. Los archivos de configuración correspondientes se encuentran en `/etc/security`. Esta sección describe brevemente los archivos de configuración relevantes para el ejemplo de sshd: `pam_unix2.conf`, `pam_env.conf`, `pam_pwcheck.conf` y `limits.conf`.

16.3.1 pam_unix2.conf

El método tradicional de autenticación basada en contraseña está controlado a través del módulo PAM `pam_unix2`. Este módulo puede leer los datos necesarios desde `/etc/passwd, /etc/shadow,` mapas NIS, tablas NIS+ o bases de datos LDAP. El comportamiento de este módulo puede manipularse configurando las opciones PAM de la aplicación en sí o bien de manera global en `/etc/security/pam_unix2.conf`. En el caso más sencillo, este archivo de configuración tiene el aspecto mostrado en el Ejemplo 16.6, “pam_unix2.conf” (p. 330).

Ejemplo 16.6 *pam_unix2.conf*

```
auth:   nullok
account:
password:       nullok
session:        none
```

La opción `nullok` de los tipos de módulos `auth` y `password` especifica que es posible incluir contraseñas vacías en el tipo de cuentas correspondiente. Los usuarios también pueden cambiar las contraseñas de sus cuentas. La opción `none` en el tipo de módulo `session` especifica que no se registran mensajes en su nombre (se trata de la opción por defecto). Puede obtener información acerca de otras opciones de configuración a través de los comentarios dentro del propio archivo y a través de la página de manual pam_unix2(8).

16.3.2 pam_env.conf

Este archivo se puede utilizar para definir un entorno estandarizado para usuarios, el cual se establecerá cada vez que se llame al módulo `pam_env`. Si se utiliza este archivo, las variables de entorno deberán predefinirse con la sintaxis siguiente:

```
VARIABLE  [DEFAULT=[valor]]  [OVERRIDE=[valor]]
```

`VARIABLE`
: Nombre de la variable de entorno que definir.

`[DEFAULT=[valor]]`
: Valor por defecto que desea definir el administrador.

`[OVERRIDE=[valor]]`
: Valores que se pueden consultar y definir mediante `pam_env`, sustituyendo al valor por defecto.

Un ejemplo típico de cómo se podría utilizar `pam_env` sería adaptar la variable `DISPLAY`, que se podría cambiar cuando se inicie sesión de forma remota. Esta situación se muestra en el Ejemplo 16.7, “pam_env.conf” (p. 331).

Ejemplo 16.7 *pam_env.conf*

```
REMOTEHOST      DEFAULT=localhost OVERRIDE=@{PAM_RHOST}
DISPLAY         DEFAULT=${REMOTEHOST}:0.0 OVERRIDE=${DISPLAY}
```

La primera línea define el valor de la variable `REMOTEHOST` en `localhost`, la cual se utilizará cada vez que `pam_env` no pueda determinar ningún otro valor. La variable `DISPLAY`, a su vez, contiene el valor de `REMOTEHOST`. Podrá obtener más información a través de los comentarios del archivo `/etc/security/pam_env.conf`.

16.3.3 pam_pwcheck.conf

Este archivo de configuración corresponde al módulo `pam_pwcheck`, que lee las opciones que incluye para todos los módulos del tipo `password`. Los ajustes almacenados en este archivo tienen preferencia sobre los ajustes PAM de una aplicación individual. Si no se han definido los ajustes específicos de la aplicación, ésta utiliza los ajustes globales. El Ejemplo 16.8, “pam_pwcheck.conf” (p. 332) le indica a `pam_pwcheck` que permita que se utilicen contraseñas vacías, así como que se modifiquen las contraseñas. El archivo `/etc/security/pam_pwcheck.conf` menciona otras opciones disponibles para el módulo.

Ejemplo 16.8 *pam_pwcheck.conf*

```
password:    nullok
```

16.3.4 limits.conf

Se pueden definir límites del sistema para usuarios o para grupos en el archivo `limits.conf`, el cual lee el módulo `pam_limits`. Este archivo le permite definir límites rígidos, que no se podrán sobrepasar en absoluto, y límites flexibles, que sí se pueden sobrepasar temporalmente. Lea los comentarios incluidos en el archivo para obtener más información sobre la sintaxis empleada y las opciones disponibles.

16.4 Información adicional

En el directorio `/usr/share/doc/packages/pam` del sistema instalado encontrará la siguiente documentación adicional:

Archivos README (LÉAME)
: El nivel superior de este directorio incluye archivos README generales. El subdirectorio `modules` tiene archivos README sobre los módulos PAM disponibles.

The Linux-PAM System Administrators' Guide (Guía del administrador del sistema Linux-PAM)
: Este documento incluye todo aquello que un administrador del sistema debería saber sobre PAM. Todo explicado a través de una amplia gama de temas, desde la sintaxis de los archivos de configuración a cuestiones de seguridad relacionadas

con los módulos PAM. Este documento está disponible en formato PDF, HTML y sólo texto.

The Linux-PAM Module Writers' Manual (Manual del desarrollador de módulos Linux-PAM)
: Este documento resume los datos desde el punto de vista del desarrollador e incluye información acerca de cómo desarrollar módulos PAM que cumplan con los estándares. El documento está disponible en formato PDF, HTML y sólo texto.

The Linux-PAM Application Developers' Guide (Guía del desarrollador de aplicaciones Linux-PAM)
: Este documento incluye todo lo que debe saber el desarrollador de aplicaciones que quiera utilizar las bibliotecas PAM. El documento está disponible en formato PDF, HTML y sólo texto.

Thorsten Kukuk ha desarrollado una serie de módulos PAM para SUSE Linux y ha dejado información al respecto en `http://www.suse.de/~kukuk/pam/`.

17 Virtualización mediante Xen

Xen hace posible ejecutar varios sistemas Linux en una máquina física. El hardware para los distintos sistemas se proporciona de forma virtual. Este capítulo ofrece una descripción general de las posibilidades y limitaciones de esta tecnología. Las secciones sobre la instalación, configuración y ejecución de Xen completan esta introducción.

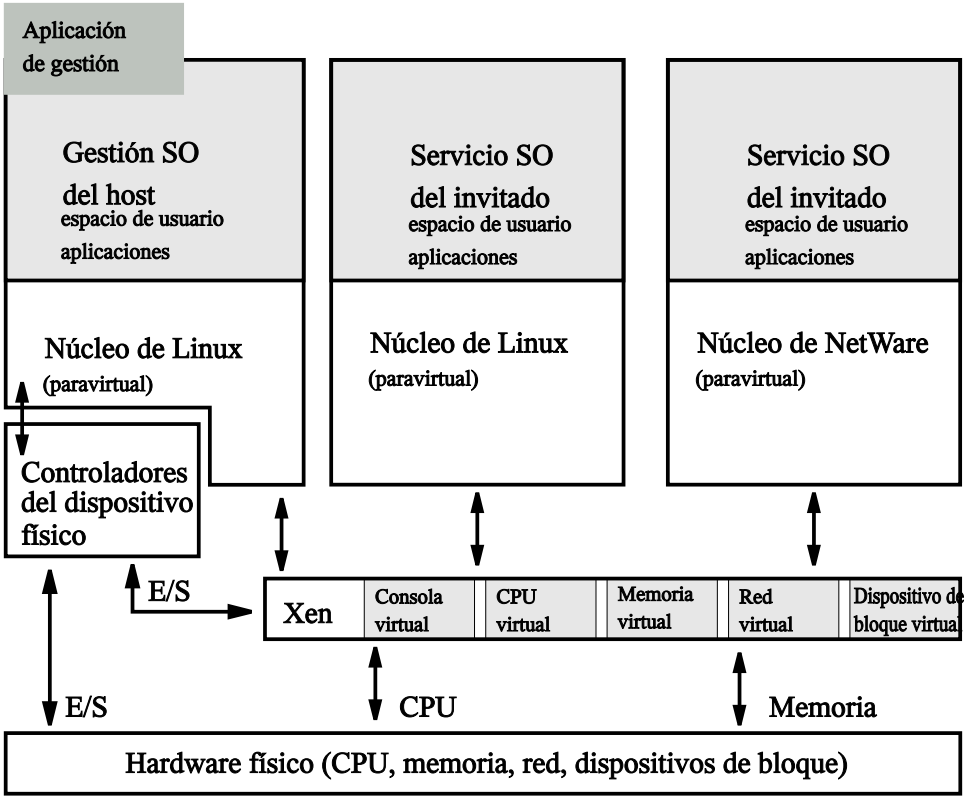
Por lo general, las máquinas virtuales necesitan imitar el hardware que un sistema necesita. El inconveniente es que el hardware emulado es mucho más lento que el real. Xen adopta una perspectiva diferente, puesto que restringe la emulación al número mínimo posible de partes. Para lograrlo, Xen utiliza la *paravirtualización*. Ésta es una técnica que presenta máquinas virtuales similares, aunque no idénticas al hardware subyacente. Por lo tanto, los sistemas operativos del host y del invitado se adaptan al nivel del núcleo. El espacio de usuario permanece sin cambios. Xen controla el hardware con un hipervisor y un invitado controlador (también denominado "dominio-0") que proporcionan los dispositivos virtuales de bloque y de red necesarios. Los sistemas invitados utilizan estos dispositivos para ejecutar el sistema y realizar la conexión con otros invitados o con la red local. Cuando varias máquinas físicas que ejecutan Xen se configuran de tal forma que los dispositivos virtuales de bloque y de red se encuentran disponibles, también resulta posible migrar un sistema invitado de un elemento de hardware a otro durante su ejecución. Originariamente, Xen se desarrolló para funcionar hasta con 100 sistemas invitados en un solo equipo; no obstante, este número presenta una fuerte dependencia de los requisitos del sistema de los sistemas invitados en ejecución (sobre todo del uso de la memoria).

Para limitar el uso de la CPU, el hipervisor de Xen ofrece tres planificadores distintos. El planificador también puede cambiarse durante la ejecución del sistema invitado, con lo que se posibilita el cambio de prioridad del sistema invitado en ejecución. En un

nivel más alto, la migración de un invitado también puede utilizarse para ajustar los recursos disponibles de la CPU.

El sistema de virtualización Xen también presenta algunas desventajas relacionadas con el hardware admitido. Hay varios controladores de código no abierto, como los de Nvidia o ATI, que no funcionan como deberían. En estos casos, deben utilizarse los controladores de origen cerrado si se encuentran disponibles, aun si no admiten todas las capacidades de los chips. Al utilizar Xen, tampoco se admiten varios chips de WLAN y bridges Cardbus. En la versión 2, Xen no admite PAE (Physical Address Extension, Extensión de dirección física), lo que significa que no admite más de 4 GB de memoria. Tampoco se admite ACPI. La gestión de energía y otros modos que dependen de la ACPI no funcionan. Otra limitación de Xen es que actualmente no es posible arrancar simplemente un dispositivo de bloque. Para arrancar siempre es necesario contar con el núcleo correcto y el initrd disponible en dominio-0.

Figura 17.1 *Descripción general de Xen*



17.1 Instalación de Xen

El procedimiento de instalación de Xen implica la configuración de un dominio de tipo dominio-0 y la instalación de invitados Xen. En primer lugar, asegúrese de que los paquetes necesarios se encuentren instalados. Son los siguientes: `python`, `bridge-utils`, `xen`, `xen-tools`, `xen-tools-ioemu` y `kernel-xen`. Al seleccionar Xen durante la instalación, Xen se añadirá a la configuración de GRUB. En otros casos, cree en `boot/grub/menu.lst` una entrada similar a la siguiente:

```
title Xen3
  kernel (hd0,0)/boot/xen.gz
  module (hd0,0)/boot/vmlinuz-xen <parámetros>
  module (hd0,0)/boot/initrd-xen
```

Sustituya (hd0,0) por la partición en la que se encuentre el directorio `/boot`. Consulte también el Capítulo 9, *Cargador de arranque* (p. 211). Sustituya <parámetros> con los parámetros que se usan normalmente para arrancar un núcleo de Linux. A continuación, rearranque en modo Xen. Esto arranca el hipervisor de Xen y un núcleo Linux ligeramente modificado como dominio-0 que ejecuta la mayor parte del hardware. Aparte de las excepciones que ya se han mencionado, todo debería funcionar normalmente.

17.2 Instalación de dominios

Cada dominio invitado debe instalarse de manera individual. Para ello, ejecute la instalación de la máquina virtual del módulo de YaST (Xen) en el grupo de software. En la interfaz siguiente, ofrezca toda la información necesaria para ejecutar el instalador. Esta información está dividida en cuatro categorías:

Options
: Defina el nombre del dominio invitado, su recurso de memoria y las opciones de arranque del instalador.

Discos
: Seleccione crear una imagen del sistema de archivos o una partición física real. Las imágenes del sistema de archivos se almacenan en el directorio `/var/lib/xen/images`. Asegúrese de que cuenta con espacio en disco suficiente en este directorio.

Sistema operativo
: Sistema operativo que debería usarse para instalar el dominio invitado. Este sistema se selecciona en el origen de la instalación del módulo de YaST y no puede definirse en este flujo de trabajo.

Red
: Este módulo sólo admite conectividad mediante bridges. Añada el número de tarjetas de red virtuales que necesite.

El siguiente cuadro de diálogo inicia el sistema de instalación después de realizar varias tareas de configuración. Este sistema es idéntico a la instalación estándar en modo de texto descrita en la Sección “YaST en modo de texto” (Capítulo 2, *Configuración del sistema con YaST*, ↑Inicio).

Si necesita cambiar la configuración de un dominio invitado, deberá hacerlo directamente en el archivo de configuración. Se encuentra en `/etc/xen` y su nombre es idéntico al del dominio invitado.

17.3 Inicio y control de los dominios Xen con xm

Xen reduce automáticamente la cantidad de memoria de dominio-0 para ajustarse a los requisitos del dominio invitado que se acaba de iniciar. Si no hay suficiente memoria disponible, no se iniciará el invitado. Siempre podrá comprobar la memoria disponible de dominio-0 con el comando `free`.

Siempre será posible desconectar una consola o volver a conectarla desde otro terminal. Para llevar a cabo la desconexión, utilice Ctrl +]. Para volver a conectarla, compruebe en primer lugar el ID del invitado necesario mediante `xm list` y realice la conexión con ese ID mediante `xm console` *`ID`*.

La herramienta xm de Xen tiene muchos parámetros posibles. Escriba `xm help` para visualizar una lista con una breve explicación. La Tabla 17.1, "Comandos xm" (p. 339) proporciona algunos de los comandos más importantes útiles como punto de partida.

Tabla 17.1 *Comandos xm*

`xm help`	Imprime una lista de los comandos disponibles para la herramienta xm.
`xm console` *`ID`*	Efectúa la conexión con la primera consola (tty1) del invitado con el ID *`ID`*.
`xm mem-set` *`ID Mem`*	Establece el tamaño de la memoria del dominio con el ID *`ID`* como *`Mem`*, expresado este último valor en MB.
`xm create` *`nombredom`* `[-c]`	Inicia el dominio con el archivo de configuración *`nombredom`*. El elemento opcional `-c` enlaza el terminal actual con el primer tty del nuevo invitado.
`xm shutdown` *`ID`*	Apaga el invitado con el ID *`ID`* de la forma habitual.

`xm destroy ID`	Finaliza inmediatamente el invitado con el ID *ID*.
`xm list`	Imprime una lista de todos los dominios en ejecución con sus IDs, memoria y valores temporales de la CPU.
`xm info`	Muestra información sobre el host Xen, incluida la relativa a la memoria y a la CPU.

17.4 Solución de problemas

Esta sección ofrece algunas sugerencias sobre cómo resolver problemas comunes. No se trata de instrucciones exhaustivas, pero deberían ayudar a resolver algunos problemas.

Problemas de conectividad en Xen3.
: El concepto de conectividad ha cambiado mucho de Xen2 a Xen3. El dominio-0 ya no está directamente conectado con el bridge para impedir que se bloquee. Desafortunadamente, los guiones de inicialización del sistema no pueden gestionar la configuración actual. Para reiniciar la red, ejecute `/etc/init.d/xend restart`.

Necesito realizar una comprobación del sistema de archivos.
: Si el sistema de archivos no ha funcionado automáticamente, podrá hacerlo manualmente desde el dominio-0. Apague el invitado y ejecute `fsck` en la imagen mientras no se monte. Si `fsck` advierte que el sistema de archivos está montado, compruebe los montajes con el comando `mount`.

DHCP no obtiene las direcciones IP.
: DHCP necesita varios módulos de núcleo iptables para funcionar. Puede ser que no se hayan instalado o que haya actualizado el núcleo pero haya olvidado actualizar los módulos del núcleo en el sistema invitado.

Hay un problema al arrancar el hipervisor y los mensajes aparecen demasiado rápido.
: Conecte el equipo con Xen a otra estación de trabajo mediante un cable serie de conexión directa. A continuación, donde esté instalado Xen, añada el parámetro siguiente a la línea:

```
kernel (hd0,0)/boot/xen.gz com1=115200,8n1
```

Antes de arrancar Xen, inicie un programa de terminal en la estación de trabajo. Por ejemplo, podría ser así:

```
screen /dev/ttyS0 115200
```

Cambie el dispositivo y la velocidad según sus necesidades.

17.5 Información adicional

Puede encontrarse más información sobre Xen en los siguientes sitios Web:

- `/usr/share/doc/packages/xen/user/html/index.html`: información oficial para los usuarios de Xen. Se necesita el paquete `xen-doc-html`.
- `/usr/share/doc/packages/xen/interface/html/index.html`: documentación técnica adicional sobre la interfaz. También se necesita el paquete `xen-doc-html`.
- `http://www.cl.cam.ac.uk/Research/SRG/netos/xen/index.html`: página inicial de Xen con varios enlaces de documentación.
- `http://lists.xensource.com/`: varias listas de correos sobre Xen.
- `http://wiki.xensource.com/xenwiki`: wiki de Xen para la comunidad de código abierto.

Parte 4. Servicios

18 Trabajo en red básico

Linux ofrece las herramientas y funciones necesarias para trabajar en red que se integran en todos los tipos de estructuras de red. El protocolo tradicional de Linux, TCP/IP, dispone de varios servicios y funciones especiales que se tratan aquí. El acceso a la red mediante una tarjeta de red, un módem u otro dispositivo se puede configurar con YaST. También es posible la configuración manual. En este capítulo, sólo se explican los mecanismos fundamentales y los archivos de configuración de red relevantes.

Linux y otros sistemas operativos de Unix utilizan el protocolo TCP/IP. No se trata de un único protocolo de red, sino de una familia de protocolos de red que ofrece varios servicios. Los protocolos enumerados en la Tabla 18.1, “Algunos protocolos de la familia de protocolos TCP/IP” (p. 346) se proporcionan con el fin de intercambiar datos entre dos máquinas mediante TCP/IP. Las redes combinadas por TCP/IP que forman una red mundial se denominan en su totalidad “Internet”.

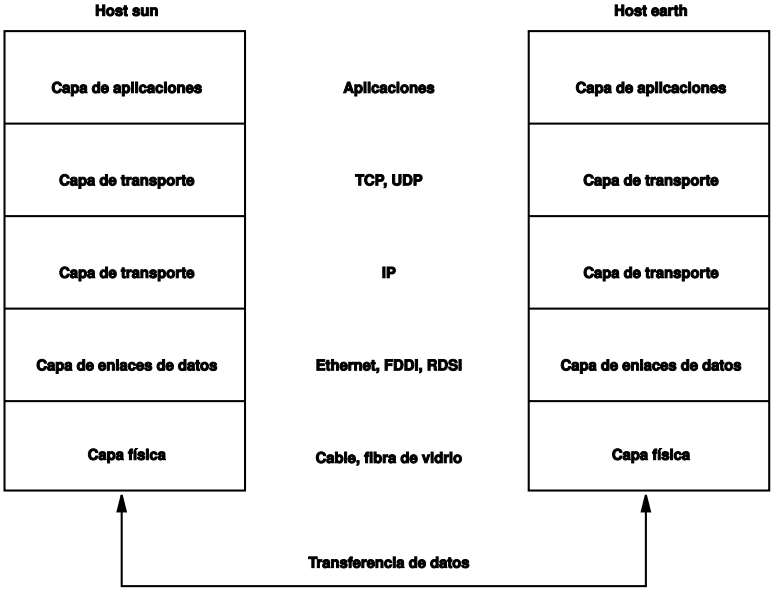
RFC significa *petición de comentario*. Las RFC (Peticiones de comentarios) son documentos que describen varios protocolos y procedimientos de implementación de Internet para el sistema operativo y sus aplicaciones. Los documentos RFC describen la configuración de los protocolos de Internet. Para ampliar sus conocimientos acerca de cualquiera de los protocolos, consulte los documentos RFC apropiados. Están disponibles en línea en la dirección `http://www.ietf.org/rfc.html`.

Tabla 18.1 *Algunos protocolos de la familia de protocolos TCP/IP*

Protocolo	Descripción
TCP	Protocolo de control de transmisión: Protocolo seguro orientado a la conexión. Los datos que se van a transmitir se envían primero a la aplicación como flujo de datos y, a continuación, el sistema operativo los convierte al formato apropiado. Los datos llegan a la aplicación correspondiente del host de destino en el formato original del flujo de datos en el que se enviaron al principio. TCP determina si se ha perdido algún dato durante la transmisión y que no se han mezclado. TCP se implementa donde la secuencia de datos es relevante.
UDP	Protocolo de datagramas de usuario: Protocolo inseguro y sin conexión. Los datos que se van a transmitir se envían en forma de paquetes generados por la aplicación. No se garantiza el orden en el que los datos llegan al destinatario y es posible que los datos se pierdan. UDP es apropiado para las aplicaciones orientadas al registro. Presenta un período de latencia menor que el TCP.
ICMP	Protocolo de mensajes de control de Internet: Fundamentalmente, no se trata de un protocolo para el usuario final, sino de un protocolo especial de control que genera informes de errores y que controla el comportamiento de las máquinas que participan en la transferencia de datos mediante TCP/IP. Además, ofrece un modo especial de eco que se puede visualizar mediante el programa ping.
IGMP	Protocolo de gestión de grupos de Internet: Este protocolo controla el comportamiento de la máquina cuando se lleva a cabo la multidifusión de IP.

Como se muestra en la Figura 18.1, “Modelo simplificado de capa para TCP/IP” (p. 347), el intercambio de datos se lleva a cabo en diferentes capas. La capa de red es la transferencia de datos insegura mediante IP (Protocolo de Internet). Además del IP, el TCP (protocolo de control de transmisión) garantiza, hasta cierto punto, la seguridad de la transferencia de datos. El protocolo subyacente que depende del hardware, como ethernet, admite la capa IP.

Figura 18.1 *Modelo simplificado de capa para TCP/IP*



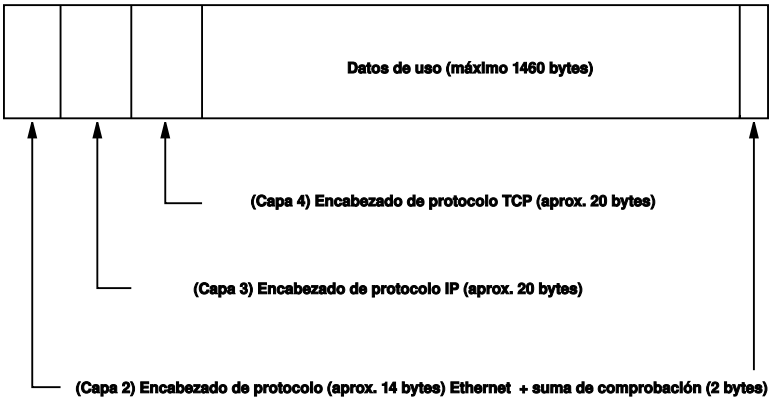
En el diagrama se ofrecen uno o dos ejemplos de cada capa. Las capas de ordenan de acuerdo con los *niveles de abstracción*. La capa inferior está íntimamente relacionada con el hardware. La capa superior, sin embargo, es casi una abstracción completa del hardware. Todas las capas tienen su propia función. Las funciones especiales de cada capa están en su mayoría implícitas en la descripción. El enlace a los datos y las capas físicas representan la red física utilizada, como ethernet.

Casi todos los protocolos de hardware funcionan por paquetes. Los datos que se van a transmitir se agrupan por *paquetes*, porque no se pueden enviar todos de una vez. El tamaño máximo de un paquete TCP/IP es aproximadamente 64 KB. Los paquetes suelen ser bastante más pequeños porque el hardware de la red puede ser un factor restrictivo. El tamaño máximo de un paquete de datos en una ethernet es aproximadamente de cien bytes. El tamaño de un paquete TCP/IP está limitado a esta cantidad cuando los datos se envían por ethernet. Si se transfieren más datos, el sistema operativo tiene que enviar más paquetes de datos.

Para que las capas cumplan las funciones designadas, se debe guardar más información relativa a cada capa en el paquete de datos. Esto se lleva a cabo en el *encabezado* del paquete. Cada capa añade un pequeño bloque de datos, denominado encabezado de protocolo, a la parte superior de cada paquete emergente. En la Figura 18.2, “Paquete

Ethernet TCP/IP" (p. 348), se muestra un paquete de datos TCP/IP de muestra que se transmite por un cable ethernet. Esta suma de prueba se ubica al final del paquete, no al principio. Esto simplifica las cosas para el hardware de red.

Figura 18.2 *Paquete Ethernet TCP/IP*



Cuando una aplicación envía datos a través de la red, los datos pasan por cada capa, todos implementados en el núcleo de Linux excepto la capa física. Cada capa se encarga de preparar los datos de modo que se puedan pasar a la siguiente capa. La capa inferior es la responsable en último lugar de enviar los datos. El procedimiento entero se invierte cuando se reciben los datos. En cada capa, los encabezados del protocolo se eliminan de los datos transportados de arriba abajo. Finalmente, la capa de transporte se encarga de hacer que los datos estén disponibles para que las aplicaciones los utilicen en el destino. De este modo, una capa sólo se comunica con la inmediatamente superior o inferior. Para las aplicaciones, no es relevante si los datos se transmiten mediante una red FDDI de 100 MBit/s o mediante una línea de módem de 56 kbit/s. De forma similar, el tipo de datos que se transmite es irrelevante para la línea de datos, siempre que los paquetes tengan el formato correcto.

18.1 Direcciones IP y encaminamiento

Esta sección está limitada a las redes IPv4. Para obtener información acerca del protocolo IPv6, sucesor de IPv4, consulte la Sección 18.2, "IPv6: Internet de la próxima generación" (p. 351).

18.1.1 Direcciones IP

Cada equipo de Internet tiene una dirección única de 32 bits. Estos 32 bits (o 4 bytes) se escriben normalmente como se ilustra en la segunda fila del Ejemplo 18.1, “Escritura de direcciones IP” (p. 349).

Ejemplo 18.1 *Escritura de direcciones IP*

```
IP Address (binary):  11000000 10101000 00000000 00010100
IP Address (decimal):      192.     168.       0.      20
```

En formato decimal, los cuatro bytes se escriben en el sistema de numeración decimal, separados por puntos. La dirección IP se asigna a un host o a una interfaz de red. No se puede utilizar en ningún sitio más. Hay excepciones a esta regla, pero éstas no son relevantes en los siguientes pasajes.

Los puntos de las direcciones IP indican el sistema jerárquico. Hasta 1990, las direcciones IP se clasificaban en clases de forma estricta. Sin embargo, se observó que este sistema era demasiado inflexible y se dejó de utilizar. Ahora se utiliza *encaminamiento sin clase* (CIDR, encaminamiento entre dominios sin clase).

18.1.2 Máscaras de red y encaminamiento

Las máscaras de red se utilizan para definir el rango de direcciones de una subred. Si dos hosts se encuentran en la misma subred, pueden llegar el uno al otro directamente, si no se encuentran en la misma subred, necesitan la dirección de una gateway que gestione todo el tráfico entre la subred y el resto del mundo. Para comprobar si dos direcciones IP se encuentran en la misma subred, UNA ambas direcciones con la máscara de red.“” Si el resultado es el mismo, las dos direcciones IP se encuentran en la misma red local. Si hay diferencias, sólo será posible acceder a la dirección IP remota y, por tanto a la interfaz remota, a través de una gateway.

Para entender cómo funciona la máscara de red, consulte el Ejemplo 18.2, “Enlace de direcciones IP a la máscara de red” (p. 350) La máscara de red consta de 32 bits que identifican qué parte de la dirección IP pertenece a la red. Todos los bits `1` marcan el bit correspondiente de la dirección IP como perteneciente a la red. Todos los bits `0` marcan los bits que se encuentran en la subred. Esto significa que cuantos más bits sean `1`, menor será la subred. Como la máscara de red consta siempre de varios bits `1` sucesivos, también es posible contar sólo el número de bits de la máscara de red. En el

Ejemplo 18.2, “Enlace de direcciones IP a la máscara de red” (p. 350), la primera red con 24 bits también se podría escribir como `192.168.0.0/24`.

Ejemplo 18.2 *Enlace de direcciones IP a la máscara de red*

```
IP address (192.168.0.20):  11000000 10101000 00000000 00010100
Netmask   (255.255.255.0):  11111111 11111111 11111111 00000000
----------------------------------------------------------------
Result of the link:         11000000 10101000 00000000 00000000
In the decimal system:           192.     168.       0.       0

IP address (213.95.15.200): 11010101 10111111 00001111 11001000
Netmask    (255.255.255.0): 11111111 11111111 11111111 00000000
----------------------------------------------------------------
Result of the link:         11010101 10111111 00001111 00000000
In the decimal system:           213.      95.      15.       0
```

Éste es otro ejemplo: todas las máquinas conectadas con el mismo cable ethernet se ubican normalmente en la misma subred, y puede accederse a ellas directamente. Incluso aunque la subred esté físicamente dividida por conmutadores o bridges, es posible acceder a estos hosts directamente.

Sólo se puede llegar a las direcciones IP externas a la subred local si se configura una gateway para la red de destino. Normalmente, sólo hay una gateway que gestiona todo el tráfico externo. Sin embargo, también es posible configurar varias gateways para subredes diferentes.

Si se ha configurado una gateway, todos los paquetes IP externos se envían a la gateway apropiada. A continuación, esta gateway trata de enviar estos paquetes del mismo modo (de host a host), hasta que llega al host de destino o hasta que se agota el TTL ("tiempo de vida") del paquete.

Tabla 18.2 *Direcciones específicas*

Tipo de dirección	Descripción
Dirección de red básica	La máscara de red UNE las direcciones de la red, como se muestra en el Ejemplo 18.2, “Enlace de direcciones IP a la máscara de red” (p. 350) en `Result`. Esta dirección no se puede asignar a todos los hosts.
Dirección de difusión	En general, esto significa “Acceder a todos los hosts de esta subred”. Para generar esto, la red se invierte en formato binario

Tipo de dirección	Descripción
	y se une a la dirección de red básica con un OR lógico. Por tanto, el ejemplo anterior da como resultado 192.168.0.255. Esta dirección no se puede asignar a todos los hosts.
Host local	La dirección `127.0.0.1` se asigna al "dispositivo de retrobucle" de cada host. Puede configurar una conexión en su propia máquina con esta dirección.

Como las direcciones IP deben ser únicas en todo el mundo, no debe seleccionar sólo direcciones aleatorias. Si desea configurar una red privada basada en IP, puede utilizar tres dominios de direcciones. Éstos no obtienen ninguna conexión del resto de Internet, porque no se pueden transmitir por Internet. Estos dominios de direcciones se especifican en RFC 1597 y se enumeran en la Tabla 18.3, "Dominios de direcciones IP privadas" (p. 351).

Tabla 18.3 *Dominios de direcciones IP privadas*

Subred/Máscara de red	Dominio
`10.0.0.0/255.0.0.0`	`10.x.x.x`
`172.16.0.0/255.240.0.0`	`172.16.x.x – 172.31.x.x`
`192.168.0.0/255.255.0.0`	`192.168.x.x`

18.2 IPv6: Internet de la próxima generación

Debido al surgimiento de la WWW (World Wide Web), Internet ha crecido de forma fulminante con un número de equipos que se comunican mediante TCP/IP que durante los últimos quince años va en constante aumento. Desde que Tim Berners-Lee, del CERN, (`http://public.web.cern.ch`) inventó la WWW en 1990, el número de hosts de Internet ha crecido de unos cientos a cien millones aproximadamente.

Como se ha mencionado, una dirección IPv4 consta sólo de 32 bits. Además, muchas direcciones IP se pierden, es decir, no se pueden usar debido a la forma en que están organizadas las redes. El número de direcciones disponibles en la subred es dos veces la capacidad del número de bits, menos dos. Una subred tiene, por ejemplo, 2, 6 ó 14 direcciones disponibles. Para conectar 128 hosts a Internet, por ejemplo, se necesita una subred con 256 direcciones IP, de las que son utilizables 254 porque se necesitan dos direcciones IP para la estructura de la subred en sí misma: la dirección de red básica y la dirección de difusión.

En el protocolo IPv4 actual, DHCP o NAT (traducción de direcciones de red) son los mecanismos típicos utilizados para eludir la posible falta de direcciones. Combinados con la convención de mantener los espacios de las direcciones públicas y de las privadas separados, estos métodos pueden mitigar la falta. El problema reside en su configuración, que es una instalación ardua y una carga que mantener. Para configurar un host en una red IPv4, se necesitan varios elementos de direcciones, como la propia dirección IP del host, la subred, la dirección de gateway y quizás la dirección de un servidor de nombres. Todos estos elementos deben conocerse y no se pueden derivar de ningún otro sitio.

Con IPv6, tanto la falta de direcciones como la configuración complicada se relegan al pasado. En las siguientes secciones se ofrece más información acerca de las mejoras y ventajas que ofrece IPv6 y acerca de la transición del protocolo antiguo al nuevo.

18.2.1 Ventajas

La mejora más importante y más visible que ofrece el protocolo nuevo es la enorme ampliación del espacio de direcciones disponible. Una dirección IPv6 está formada por valores de 128 bits en lugar de los 32 bits tradicionales. Esto proporciona varios cuatrillones de direcciones IP.

Sin embargo, las direcciones IPv6 no son diferentes de sus predecesoras en cuanto a la longitud. También tienen una estructura interna diferente que puede contener más información específica acerca de los sistemas y de las redes a las que pertenecen. En la Sección 18.2.2, “Tipos de direcciones y estructura” (p. 354) encontrará más información acerca de esto.

A continuación, se muestra una lista con algunas otras ventajas del nuevo protocolo:

Configuración automática
: IPv6 proporciona a la red una capacidad “plug and play”, lo que significa que un sistema configurado recientemente se integra en la red local sin que haya que configurarlo de forma manual. El host nuevo utiliza el mecanismo de configuración automática para extraer su propia dirección a partir de la información que los routers vecinos ponen a su disposición, mediante un protocolo denominado protocolo ND *descubrimiento de vecino*. Este método no requiere intervención por parte del administrador y no es necesario mantener un servidor central para asignar direcciones (una ventaja adicional respecto al IPv4), donde la asignación automática de direcciones requiere un servidor DHCP.

Movilidad
: IPv6 hace posible asignar varias direcciones a una interfaz de red al mismo tiempo. Esto permite a los usuarios acceder a varias redes fácilmente, algo que podría compararse con los servicios internacionales de itinerancia que ofrecen las compañías de telefonía móvil: si lleva el teléfono móvil al extranjero, el teléfono se registra en un servicio de dicho país en cuanto entra en el área correspondiente, de modo que podrá llamar y recibir llamadas desde el mismo número en todas partes, como si estuviera en su país.

Comunicación segura
: Con IPv4, la seguridad de la red es una función complementaria. IPv6 incluye IPSec como una de sus funciones principales, lo que permite que los sistemas se comuniquen a través de un túnel de seguridad para evitar que los intrusos vean la información en Internet.

Compatibilidad inversa
: Para ser realistas, sería imposible cambiar todo Internet de IPv4 a IPv6 a la vez. Por tanto, es fundamental que los dos protocolos puedan coexistir no sólo en Internet, sino también en un sistema. Esto se garantiza con direcciones compatibles (las direcciones IPv4 se pueden traducir en direcciones IPv6) y con el uso de varios túneles. Consulte la Sección 18.2.3, “Coexistencia de IPv4 y IPv6” (p. 358). Además, los sistemas se pueden basar en una técnica de *IP de stack dual* para admitir los dos protocolos al mismo tiempo, lo que significa que tienen dos stacks de red completamente separados, de modo que no hay interferencias entre las dos versiones del protocolo.

Servicios personalizados mediante multidifusión
: Con IPv4, algunos servicios como MIB tienen que difundir los paquetes a todos los hosts de la red local. IPv6 permite un enfoque mucho más preciso al habilitar

los servidores para dirigirse a los hosts mediante la *multidifusión*, es decir, llegando a varios hosts como partes de un grupo (lo que es diferente de llegar a todos a través de la *difusión* o a cada host por separado a través de la *monodifusión*). Los hosts a los que se llega como grupo pueden depender de la aplicación en concreto. Hay algunos grupos predefinidos para llegar a todos los servidores de nombres (el *grupo de multidifusión a todos los servidores de nombres*), por ejemplo, o a todos los routers (el *grupo de multidifusión a todos los routers*).

18.2.2 Tipos de direcciones y estructura

Como ya se ha mencionado, el protocolo IP actual tiene dos deficiencias importantes: cada vez faltan más direcciones IP y la configuración de la red y el mantenimiento de las tablas de encaminamiento son tareas cada vez más complejas y costosas. IPv6 soluciona el primer problema ampliando el espacio de las direcciones hasta 128 bits. El segundo se contrarresta introduciendo una estructura jerárquica de direcciones, combinada con sofisticadas técnicas para asignar direcciones de red, además de *multinodo* (capacidad de asignar varias direcciones a un dispositivo, lo que proporciona acceso a varias redes).

Al utilizar IPv6, resulta útil conocer tres tipos de direcciones diferentes:

Monodifusión
: Las direcciones de este tipo se asocian exactamente a una interfaz de red. Los paquetes con una dirección de este tipo se entregan sólo a un destino. Por tanto, las direcciones de monodifusión se utilizan para transferir paquetes a hosts por separado en la red local o en Internet.

Multidifusión
: Las direcciones de este tipo están relacionadas con un grupo de interfaces de red. Los paquetes con direcciones de ese tipo se entregan en todos los destinos que pertenecen al grupo. Las direcciones de multidifusión las utilizan principalmente algunos servicios de red para comunicarse con ciertos grupos de hosts de una forma precisa.

Cualquier difusión
: Las direcciones de este tipo están relacionadas con un grupo de interfaces. Los paquetes con una dirección de ese tipo se entregan al miembro del grupo más cercano al remitente, de acuerdo con los principios del protocolo subyacente de encaminamiento. Las direcciones de cualquier difusión se utilizan para facilitar

que los hosts encuentren servidores que ofrezcan ciertos servicios en el área de red en cuestión. Todos los servidores del mismo tipo tienen la misma dirección de cualquier difusión. Siempre que un host solicita un servicio, recibe una respuesta del servidor más cercano, como determina el protocolo de encaminamiento. Si por algún motivo el servidor fallara, el protocolo selecciona de forma automática el segundo servidor más cercano, a continuación, el tercero, etc.

Una dirección IPv6 está formada por ocho campos de cuatro dígitos, cada uno de los cuales representa 16 bits escritos en notación hexadecimal. También se separan mediante dos puntos (`:`). Los bytes de ceros situados al principio de un campo se pueden eliminar, pero los ceros del campo o del final, no. Otra convención es que más de cuatro bytes consecutivos de ceros se pueden colapsar en dos signos de dos puntos. Sin embargo, sólo se permite `::` por dirección. Este tipo de notación abreviada se muestra en el Ejemplo 18.3, "Dirección IPv6 de muestra" (p. 355), donde las tres líneas representan la misma dirección.

Ejemplo 18.3 *Dirección IPv6 de muestra*

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                           : 10 : 1000 : 1a4
```

Cada parte de una dirección IPv6 tiene una función definida. Los primeros bytes forman el prefijo y especifican el tipo de dirección. La parte central es la parte de red de la dirección, pero puede no utilizarse. El final de la dirección forma la parte del host. Con IPv6, la máscara de red se define indicando la longitud del prefijo después de una barra al final de la dirección. Una dirección, como se muestra en el Ejemplo 18.4, "Dirección IPv6 encargada de especificar la longitud del prefijo" (p. 355), contiene información para que los primeros 64 bits formen la parte de red de la dirección y para que los últimos 64 formen la parte del host. En otras palabras, el `64` significa que la máscara de red se rellena con 64 valores de 1 bit de izquierda a derecha. Al igual que sucede con IPv4, la dirección IP se combina con AND con los valores de la máscara de red para determinar si el host se ubica en la misma red o en otra.

Ejemplo 18.4 *Dirección IPv6 encargada de especificar la longitud del prefijo*

```
fe80::10:1000:1a4/64
```

IPv6 reconoce varios tipos predefinidos de prefijos. Algunos de ellos se muestran en la Tabla 18.4, "Varios prefijos IPv6" (p. 356).

Tabla 18.4 *Varios prefijos IPv6*

Prefijo (hex.)	Definición
`00`	Direcciones de compatibilidad para direcciones IPv4 y para direcciones IPv4 sobre IPv6. Éstas se utilizan para mantener la compatibilidad con IPv4, pero, para utilizarlas, sigue siendo necesario un router con capacidad para traducir paquetes IPv6 en paquetes IPv4. Varias direcciones especiales, como la del dispositivo de retrobucle, también tienen este prefijo.
`2` ó `3` como primer dígito	Direcciones globales de monodifusión agregables. Como sucede con IPv4, se puede asignar una interfaz para que forme parte de una cierta subred. Actualmente, existen los siguientes espacios de direcciones: `2001::/16` (espacio de dirección de calidad de producción) y `2002::/16` (espacio de direcciones 6to4).
`fe80::/10`	Direcciones locales de enlace. Las direcciones con este prefijo no deberían encaminarse y, por tanto, sólo se debería llegar a ellas desde la misma subred.
`fec0::/10`	Direcciones locales de sitio. Éstas se pueden encaminar, pero sólo en la red de la organización a la que pertenecen. En efecto, son el equivalente de IPv6 del espacio actual de direcciones de red privada, como `10.x.x.x`.
`ff`	Éstas son direcciones de multidifusión.

Una dirección de monodifusión consiste en tres componentes básicos:

Topología pública
: La primera parte (que contiene también uno de los prefijos mencionados anteriormente) se utiliza para encaminar paquetes a través de Internet. Incluye información acerca de la compañía o de la institución que proporciona el acceso a Internet.

Topología del sitio
: La segunda parte contiene información de encaminamiento acerca de la subred en la que se va a entregar el paquete.

ID de interfaz
: La tercera parte identifica la interfaz en la que se va a entregar el paquete. Esto también permite que el identificador MAC forme parte de la dirección. Como el MAC es un identificador único y flexible codificado en el dispositivo por el fabricante de hardware, el procedimiento de configuración se simplifica de forma sustancial. De hecho, los primeros 64 bits de las direcciones se consolidan para formar el testigo `EUI-64`. De ellos, los últimos 48 bits se toman del MAC y los 24 restantes contienen información especial acerca del tipo de testigo. Esto también hace que sea posible asignar un testigo `EUI-64` a las interfaces que no disponen de un MAC, como las basadas en PPP o en RDSI.

Además de esta estructura básica, IPv6 distingue entre cinco tipos diferentes de direcciones de monodifusión:

`::` (no especificada)
: El host utiliza esta dirección como dirección de origen cuando la interfaz se inicializa por primera vez, cuando la dirección no se puede determinar por otros medios.

`::1` (retrobucle)
: Dirección del dispositivo de retrobucle.

Direcciones compatibles con IPv4
: La dirección IPv6 está formada por la dirección IPv4 y un prefijo que consiste en 96 bits cero. Este tipo de dirección de compatibilidad se utiliza para formar túneles (consulte la Sección 18.2.3, “Coexistencia de IPv4 y IPv6” (p. 358)) para permitir que los hosts IPv4 y IPv6 se comuniquen con otros que funcionan en un entorno IPv4 puro.

Direcciones IPv4 asignadas a IPv6
: Este tipo de dirección especifica una dirección IPv4 pura en notación IPv6.

Direcciones locales
: Éstos son dos tipos de direcciones para uso local:

  local de enlace
  : Este tipo de dirección sólo se puede utilizar en la subred local. Los paquetes con una dirección de origen o de destino de este tipo no deberían encaminarse a Internet ni a otras subredes. Estas direcciones contienen un prefijo especial (`fe80::/10`) y el ID de interfaz de la tarjeta de red, cuya parte central consiste en bytes ceros. Las direcciones de este tipo se utilizan durante la configuración automática para comunicarse con otros hosts que pertenecen a la misma subred.

local de sitio
: Los paquetes que tienen este tipo de dirección se pueden encaminar a otras subredes, pero no a Internet: deben permanecer dentro de la propia red de la organización. Dichas direcciones se utilizan para las intrarredes y son un equivalente del espacio de direcciones privadas definido por IPv4. Contienen un prefijo especial (`fec0::/10`), el ID de interfaz y un campo de 16 bits que especifica el ID de subred. De nuevo, el resto se rellena con bytes ceros.

IPv6 introduce una función completamente nueva que consiste en que cada interfaz de red consigue normalmente varias direcciones IP, con la ventaja de que se puede acceder a varias redes a través de la misma interfaz. Una de estas redes se puede configurar de forma completamente automática mediante el MAC y un prefijo conocido que hace que se pueda llegar a todos los hosts de la red local en cuanto se habilita IPv6 (mediante la dirección local de enlace). Cuando el MAC forma parte de la dirección, ésta es única en el mundo. Las únicas partes variables de la dirección son las que especifican la *topología del sitio* y la *topología pública*, en función de la red en la que funcione el host.

Para que un host retroceda y avance entre redes diferentes, necesita al menos dos direcciones. Una de ellas, la *dirección personal*, no sólo contiene el ID de interfaz, sino también un identificador de la red personal a la que pertenece normalmente (y el prefijo correspondiente). La dirección personal es una dirección estática y, como tal, no suele cambiar. Aún así, todos los paquetes destinados al host móvil se le pueden entregar, independientemente de si funciona en la red personal o fuera de ella. Esto es posible gracias a las funciones completamente nuevas introducidas con IPv6 como la *configuración automática sin estado* y el *descubrimiento de vecino*. Además de la dirección personal, un host móvil consigue una o varias direcciones adicionales que pertenecen a las redes externas en las que está en itinerancia. Éstas se denominan direcciones *de auxilio*. La red personal tiene un componente que envía los paquetes destinados al host cuando está en itinerancia. En un entorno IPv6, esta tarea la lleva a cabo el *agente personal*, que lleva todos los paquetes destinados a la dirección personal y los transmite a través de un túnel. Por otro lado, los paquetes destinados a la dirección de auxilio se transfieren directamente al host móvil sin ninguna desviación especial.

18.2.3 Coexistencia de IPv4 y IPv6

La migración de todos los hosts conectados a Internet de IPv4 a IPv6 es un proceso gradual. Los dos protocolos coexistirán durante algún tiempo. La coexistencia en un sistema se garantiza donde se produce una implementación de *stack dual* en los dos

protocolos. Aún queda pendiente la cuestión de cómo debería comunicarse un host habilitado con IPv6 con un host IPv4 y cómo deberían transportarse los paquetes IPv6 por las redes actuales, que normalmente están basadas en IPv4. Las mejores soluciones ofrecen túneles y direcciones de compatibilidad (consulte la Sección 18.2.2, “Tipos de direcciones y estructura” (p. 354)).

Los hosts IPv6 más o menos aislados en la red (mundial) IPv4 se pueden comunicar a través de túneles: Los paquetes IPv6 se agrupan como paquetes IPv4 para desplazarlos a través de una red IPv4. Dicha conexión entre dos hosts IPv4 se denomina *túnel*. Para lograrlo, los paquetes deben incluir la dirección de destino IPv6 (o el prefijo correspondiente) y la dirección IPv4 del host remoto situado en el extremo receptor del túnel. Un túnel básico se puede configurar de forma manual con un acuerdo entre administradores de los hosts. También se denomina *túnel estático*.

Sin embargo, la configuración y el mantenimiento de los túneles estáticos suelen llevar demasiado trabajo como para utilizarlos en la comunicación diaria. Por tanto, IPv6 proporciona tres métodos diferentes de *túnel dinámico*:

6over4
: Los paquetes IPv6 se agrupan de forma automática como paquetes IPv4 y se envían a través de una red IPv4 con capacidad de multidifusión. IPv6 se truca para ver la red entera (Internet) como una red de área local enorme (LAN). Esto hace posible determinar el extremo receptor del túnel IPv4 de forma automática. Sin embargo, el proceso de escalación de este método no es demasiado sencillo y se ve dificultado por el hecho de que la difusión múltiple IP está poco extendida en Internet. Por tanto, sólo proporciona una solución para redes corporativas o institucionales más pequeñas en las que se puede habilitar la multidifusión. Las especificaciones para este método se exponen en RFC 2529.

6to4
: Con este método, las direcciones IPv4 se generan de forma automática a partir de direcciones IPv6, lo que permite a los hosts IPv6 comunicarse a través de una red IPv4. Sin embargo, se han detectado varios problemas relativos a la comunicación entre hosts IPv6 aislados e Internet. El método se describe en RFC 3056.

Tunnel Broker para IPv6
: Este método se lleva a cabo en servidores especiales que proporcionan túneles específicos para los hosts IPv6. Se describe en RFC 3053.

IMPORTANTE: Iniciativa 6bone

Como vestigio del “antiguo” Internet, ya existe una red distribuida en todo el mundo de subredes IPv6 conectadas mediante túneles. Ésta es la red *6bone* (`http://www.6bone.net`), un entorno de prueba IPv6 que los programadores y los proveedores de Internet pueden utilizar para desarrollar y ofrecer servicios basados en IPv6 y adquirir la experiencia necesaria para implementar el nuevo protocolo. Encontará más información en el sitio de Internet del proyecto.

18.2.4 Configuración de IPv6

Para configurar IPv6, normalmente no es necesario realizar cambios en cada estación de trabajo. Sin embargo, se debe cargar la compatibilidad con IPv6. Para hacerlo, introduzca `modprobe ipv6` como `root`.

Gracias al concepto de configuración automática de IPv6, a la tarjeta de red se le asigna una dirección en la red *local de enlace*. Normalmente, en las estaciones de trabajo no se lleva a cabo la gestión de tablas de encaminamiento. La estación de trabajo puede consultar a los routers de red, mediante el *protocolo de anuncio de servicios*, qué prefijo y gateways deberían implementarse. El programa radvd se puede utilizar para configurar un router IPv6. Este programa informa a las estaciones de trabajo acerca de qué prefijo y qué routers se deben utilizar para las direcciones IPv6. Como alternativa, utilice zebra para la configuración automática de las direcciones y del encaminamiento.

Consulte la página Man de ifup(8) para obtener información acerca de cómo configurar varios tipos de túneles mediante los archivos `/etc/sysconfig/network`.

18.2.5 Información adicional

La descripción anterior no explica el IPv6 exhaustivamente. Para obtener información más detallada acerca del nuevo protocolo, consulte la siguiente documentación en línea y los siguientes libros:

`http://www.ngnet.it/e/cosa-ipv6.php`
: Serie de artículos que proporciona una introducción bien escrita a los aspectos fundamentales de IPv6. Buen manual para obtener las nociones básicas.

`http://www.bieringer.de/linux/IPv6/`
: Aquí encontrará la ayuda de Linux IPv6 y muchos enlaces relacionados con el tema.

`http://www.6bone.net/`
: Visite este sitio si desea entrar a formar parte de una red IPv6 con túneles.

`http://www.ipv6.org/`
: Punto de partida para todo lo relacionado con IPv6.

RFC 2640
: RFC fundamental acerca de IPv6.

IPv6 Essentials
: Un libro que describe todos los aspectos importantes del asunto es *IPv6 Essentials*, escrito por Silvia Hagen (ISBN 0-596-00125-8).

18.3 Resolución de nombres

DNS ayuda a asignar una dirección IP a uno o varios nombres y a asignar un nombre a una dirección IP. En Linux, esta conversión la suele llevar a cabo un tipo especial de software denominado "Bind". La máquina que se encarga de esta conversión se denomina *servidor de nombres*. Los nombres forman un sistema jerárquico en el que el componente de cada nombre se separa mediante puntos. La jerarquía de nombres es, sin embargo, independiente de la jerarquía de direcciones IP descrita anteriormente.

Tomemos como ejemplo un nombre completo, como `earth.example.com`, escrito en formato `hostname.domain`. Un nombre completo, denominado *FDQN* (Nombre de dominio completo), consiste en un nombre de host y un nombre de dominio (`example.com`). El último incluye también el *dominio de nivel superior* o TLD (`com`).

Por razones históricas, la asignación de TLD se ha convertido en algo bastante confuso. Tradicionalmente, los nombres de dominios de tres letras se utilizan en EE.UU. En el resto del mundo, el estándar son los códigos nacionales ISO de dos letras. Además de esto, en 2000 se introdujeron TLDs mayores que representan ciertas esferas de actividad (por ejemplo, `.info`, `.name`, `.museum`).

En los comienzos de Internet (antes de 1990), el archivo `/etc/hosts` se utilizó para almacenar los nombres de todas las máquinas representadas en Internet. Esto resultó

ser poco práctico debido al creciente número de equipos conectados a Internet. Por esta razón, se desarrolló una base de datos descentralizada para almacenar los nombres de hosts de un modo ampliamente distribuido. Esta base de datos, similar al servidor de nombres, no tiene los datos que pertenecen a todos los hosts de Internet disponibles, pero puede enviar peticiones a otros servidores de nombres.

La parte superior de la jerarquía la ocupan los *servidores de nombres de root*. Estos servidores de nombres de root gestionan los dominios del nivel superior y se ejecutan en el NIC (Centro de información de red). Cada servidor de nombres de root reconoce los servidores de nombres encargados de un dominio de nivel superior dado. La información acerca de los NIC de dominios de nivel superior está disponible en la dirección `http://www.internic.net`.

DNS puede hacer más que simplemente resolver nombres de host. El servidor de nombres también reconoce qué host recibe mensajes de correo electrónico para un dominio entero (*intercambiador de correo (MX)*.

Para que la máquina resuelva una dirección IP, debe reconocer al menos un servidor de nombres y sus direcciones IP. Especifique de forma sencilla un servidor de nombres con la ayuda de YaST. Si dispone de una conexión de marcación por módem, puede que no tenga que configurar un servidor de nombres de forma manual. El protocolo de marcación proporciona la dirección del servidor de nombres a medida que se realiza la conexión. La configuración del acceso del servidor de nombres con SUSE Linux se describe en el Capítulo 20, *Sistema de nombres de dominio (DNS)* (p. 397).

El protocolo `whois` está íntimamente relacionado con DNS. Con este programa, encontrará rápidamente quién es el responsable de un dominio en cuestión.

18.4 Configuración de una conexión de red de con YaST

Linux es compatible con muchos tipos de red. La mayoría utiliza nombres de dispositivo diferentes y sus archivos de configuración están repartidos por diferentes ubicaciones del sistema de archivos. Para ver una descripción general de los diferentes aspectos de la configuración manual de redes, consulte la Sección 18.6, “Configuración manual de una conexión de red” (p. 377).

Durante la instalación, se puede utilizar YaST para configurar automáticamente todas las interfaces que se hayan detectado. El resto del hardware se puede configurar en cualquier momento después de la instalación en el sistema instalado. En las siguientes secciones se describe la configuración de la red para todos los tipos de conexiones de red admitidos por SUSE Linux.

18.4.1 Configuración de la tarjeta de red de con YaST

Después de iniciar el módulo, YaST muestra un cuadro de diálogo de configuración general de la red. Seleccione si desea utilizar YaST o NetworkManager para gestionar todos los dispositivos de red. Para utilizar NetworkManager, active *Controlada por el usuario mediante NetworkManager.* Encontrará más información acerca de NetworkManager en la Sección 18.5, “Gestión de conexiones de red con NetworkManager” (p. 374). Si desea configurar la red mediante el método tradicional con YaST, seleccione *Método tradicional con ifup.*

La parte superior de la configuración tradicional muestra una lista con todas las tarjetas de red disponibles para la configuración. Las tarjetas de red detectadas correctamente aparecen con su nombre. Los dispositivos que no se han podido detectar pueden configurarse usando *Añadir,* tal y como se describe en “Configuración manual de una tarjeta de red no detectada” (p. 363). Configure una nueva tarjeta de red o cambie la configuración existente.

Configuración manual de una tarjeta de red no detectada

La configuración de una tarjeta de red que no se ha detectado incluye los elementos siguientes:

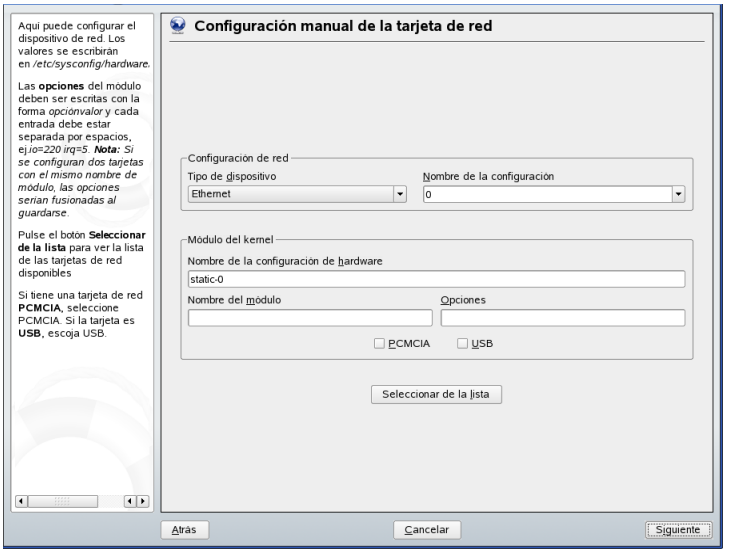
Configuración de red
: Seleccione el tipo de dispositivo de la interfaz de entre las opciones disponibles y establezca el nombre de la configuración. Encontrará información sobre las convenciones de nomenclatura de los nombres de configuración en la página Man de `getcfg(8)`.

Módulo del kernel

Nombre de la configuración de hardware especifica el nombre del archivo `/etc/sysconfig/hardware/hwcfg-*` que contiene los ajustes de hardware de la tarjeta de red. En el se indica el nombre del módulo del núcleo adecuado así como las opciones necesarias para inicializar el hardware. Normalmente, YaST sugiere nombres útiles para hardware PCMCIA y USB. Para el resto de hardware, `hwcfg-static-0` sólo tiene sentido si la tarjeta se ha configurado con el nombre de configuración `0`.

Si la tarjeta de red es un dispositivo PCMCIA o USB, active las casillas de verificación correspondientes y salga del cuadro de diálogo mediante *Siguiente*. En caso contrario, seleccione el modelo de la tarjeta de red con *Seleccionar de la lista*. YaST seleccionará automáticamente el módulo del núcleo adecuado para la tarjeta. Salga del cuadro de diálogo mediante *Siguiente*.

Figura 18.3 *Configuración de la tarjeta de red*



Configuración de la dirección de red

Seleccione el tipo de dispositivo de la interfaz y establezca el nombre de la configuración. Seleccione el tipo de dispositivo de entre los ofrecidos. Especifique un nombre de configuración según sus necesidades. No obstante, los ajustes por defecto sirven y se

pueden aceptar. Encontrará información sobre las convenciones de nomenclatura de los nombres de configuración en la página Man de `getcfg(8)`.

Si ha seleccionado *Wireless* (Inalámbrico) como tipo de dispositivo de la interfaz, configure el modo de funcionamiento, el nombre de la red (ESSID) y el cifrado en el siguiente cuadro de diálogo, *Configuración de la tarjeta de red inalámbrica*. Haga clic en *Aceptar* para completar la configuración de la tarjeta. En la Sección 34.1.3, “Configuración con YaST” (p. 655) se ofrece una descripción detallada de la configuración de tarjetas WLAN. Para los demás tipos de interfaz, continúe con la configuración de la dirección de red:

Automatic Address Setup (via DHCP) (Configuración automática de direcciones (mediante DHCP))
: Si la red cuenta con un servidor DHCP, puede delegar en él para que configure automáticamente la dirección de red. También se debe seleccionar esta opción si se utiliza una línea DSL pero el ISP no le asigna una IP estática. Si decide utilizar DHCP, seleccione *Opciones del cliente DHCP* y configure los detalles. Especifique si el servidor DHCP debería responder siempre a las peticiones y el identificador que debe utilizarse. Por defecto, los servidores DHCP utilizan la dirección de hardware de la tarjeta para identificar una interfaz. Si existe una configuración de host virtual en la que varios hosts se comunican por medio de la misma interfaz, será necesario un identificador para distinguirlos.

Configuración de la dirección estática
: Si dispone de una dirección estática, habilite esta opción. A continuación, introduzca la dirección y la máscara de subred de la red. La máscara de subred predefinida suele ser adecuada para las necesidades de una red doméstica típica.

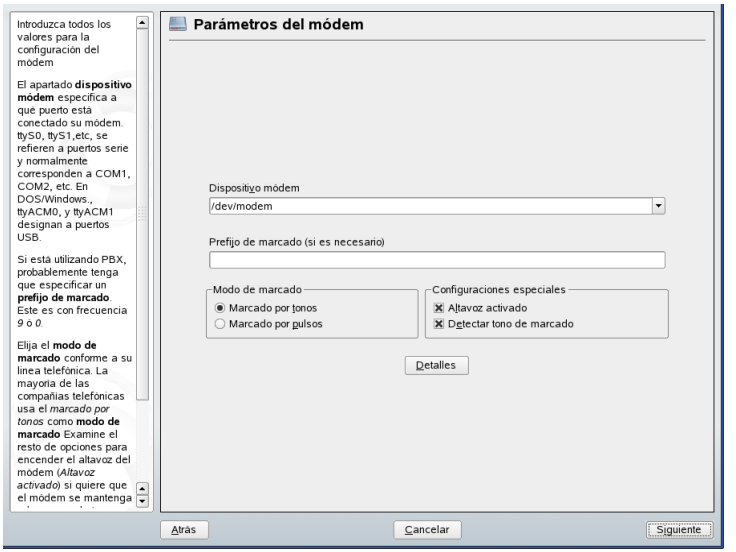
Abandone el cuadro de diálogo seleccionando *Siguiente* o continúe con la configuración del nombre de host, el servidor de nombres y los detalles de encaminamiento (consulte Servidor DNS (↑Inicio) y Enrutado (↑Inicio)).

Avanzado permite especificar ajustes más complejos. En *Configuración detallada*, utilice *Controlada por el usuario* para delegar el control de la tarjeta de red del administrador (usuario `root`) al usuario normal. En movilidad, esto permite que el usuario se adapte a los cambios en las conexiones de red de una manera más flexible, ya que puede controlar la activación y la desactivación de la interfaz. En este cuadro de diálogo también pueden establecerse la MTU (maximum transmission unit) (unidad máxima de transmisión) y el tipo de *Activación del dispositivo*.

18.4.2 Módem

En el Centro de control de YaST, acceda a la configuración del módem en *Dispositivos de red*. Si el módem no se ha detectado automáticamente, abra el cuadro de diálogo de configuración manual. En el cuadro de diálogo que se abrirá, introduzca en la interfaz a la que está conectado el módem en *Módem*.

Figura 18.4 *Configuración del módem*



Si se encuentra tras una centralita (PBX), es posible que sea necesario introducir un prefijo de marcado. A menudo, se trata de un cero. Consulte las instrucciones de la centralita para averiguarlo. Seleccione también si se utilizará marcado por tonos o por impulsos, si el altavoz debe estar conectado y si el módem debe esperar hasta que detecte el tono de marcado. No debe habilitarse esta última opción si el módem está conectado a una centralita.

En *Detalles*, establezca la velocidad en baudios y las cadenas de inicialización del módem. Cambie estos ajustes sólo si el módem no se ha detectado automáticamente o si son necesarios ajustes especiales para que funcione la transmisión de datos. Este es en general el caso de los adaptadores de terminal RDSI. Salga del cuadro de diálogo haciendo clic en *Aceptar*. Para delegar el control del módem en el usuario normal sin permisos de usuario root, active *Controlado por el usuario*. Así, un usuario sin permisos

de administrador puede activar y desactivar la interfaz. En *Expresión regular para el prefijo de marcado*, especifique una expresión regular. El *Prefijo de marcado* de KInternet, que puede ser modificado por el usuario, debe coincidir con esta expresión regular. Si el campo se deja vacío, el usuario no podrá definir otro *Prefijo de marcado* sin permisos de administrador.

En el siguiente cuadro de diálogo, seleccione el ISP (Internet service provider) (proveedor de servicios de Internet). Para escogerlo de entre una lista predefinida de IPS que operan en su país, seleccione *País*. Como alternativa, haga clic en *Nuevo* para abrir un cuadro de diálogo e introducir los datos de su ISP. Esto incluye un nombre para la conexión de acceso telefónico y el ISP además del nombre de usuario y la contraseña proporcionados por el ISP. Habilite *Pedir siempre la contraseña* para que se pida siempre la contraseña al conectar.

En el último cuadro de diálogo, especifique las opciones de conexión adicionales.

Llamada bajo demanda
: Si habilita la llamada bajo demanda, establezca al menos un servidor de nombres.

Modificar DNS si conectado
: Esta opción se encuentra habilitada por defecto; como resultado, la dirección del servidor de nombres se actualiza cada vez que se realiza la conexión a Internet.

Obtención automática de DNS
: Si el proveedor no transmite su servidor de nombres de dominio al conectar, desactive esta opción e introduzca manualmente los datos del DNS.

Modo estúpido
: Esta opción está habilitada por defecto. Con ella, no se tienen en cuenta las solicitudes de entrada enviadas por el servidor del ISP para evitar que interfieran con el proceso de conexión.

Interfaz externa del cortafuegos y *Reiniciar cortafuegos*
: La selección de estas opciones habilita SUSEfirewall2, el cual ofrece protección ante ataques externos durante la conexión a Internet.

Tiempo de inactividad (segundos)
: Especifique mediante esta opción el periodo de inactividad de la red tras el cual el módem se desconectará automáticamente.

IP Details (Detalles IP)

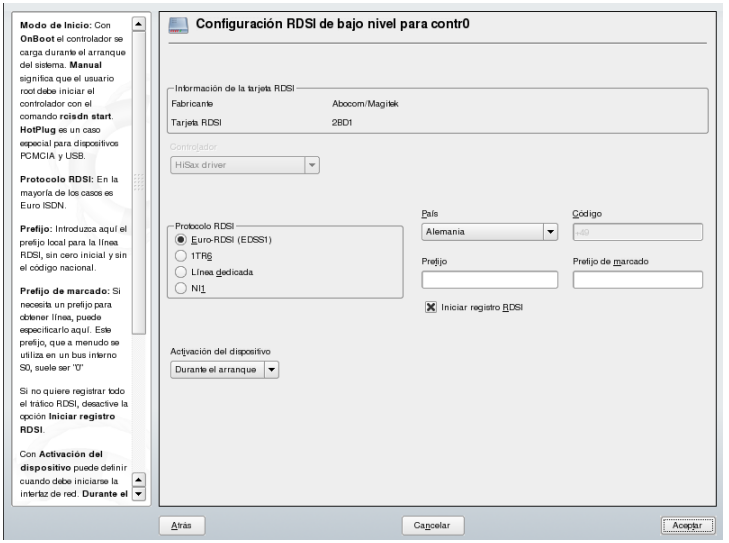
Esto abre el cuadro de diálogo de configuración de la dirección. Si el ISP no asigna una dirección IP dinámica al host, desactive *Dirección IP dinámica* e introduzca la dirección IP del host local y la dirección IP remota. Solicite esta información al ISP. Deje *Ruta predeterminada* habilitada y cierre el cuadro de diálogo seleccionando *Aceptar*.

Con *Siguiente* se vuelve al cuadro de diálogo original, que muestra un resumen de la configuración del módem. Cierre el cuadro de diálogo con *Finalizar*.

18.4.3 RDSI

Este módulo se utiliza para configurar una o varias tarjetas RDSI para el sistema. Si YaST no ha detectado la tarjeta RDSI, selecciónela manualmente. Son posibles múltiples interfaces, pero se pueden configurar varios ISP para una interfaz. En los cuadros de diálogo siguientes, establezca las opciones RDSI necesarias para el funcionamiento adecuado de la tarjeta.

Figura 18.5 *Configuración de RDSI*



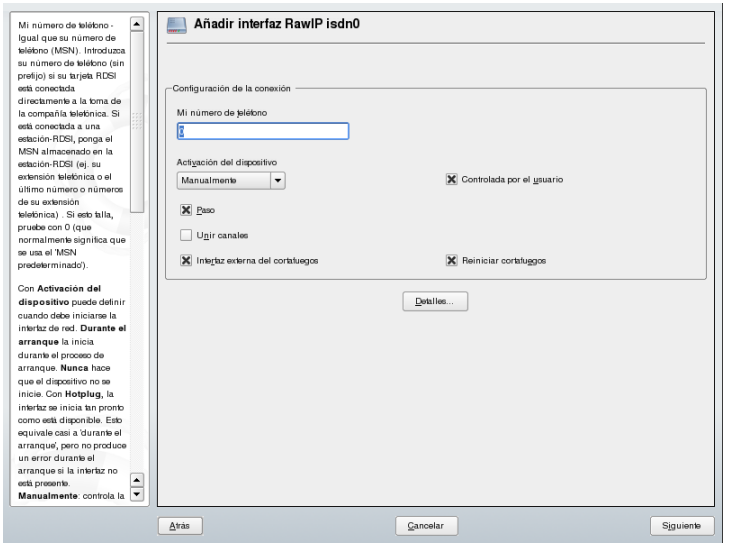
En el siguiente cuadro de diálogo, que se muestra en la Figura 18.5, “Configuración de RDSI” (p. 368), seleccione el protocolo que se utilizará. La opción por defecto es *Euro-*

ISDN (EDSS1), pero para centralitas grandes o antiguas, seleccione *1TR6*. Si se encuentra en los Estados Unidos, seleccione *NI1*. Seleccione su país en el campo correspondiente. El código del país aparecerá en el campo adyacente. Por último, introduzca el *Prefijo* y el *Prefijo de marcado* si es necesario.

Modo de inicio define cómo debe iniciarse la interfaz RDSI: *Durante el arranque* hace que el controlador RDSI se inicialice cada vez que arranque el sistema. *Manualmente* le solicita que cargue el controlador RDSI como usuario `root` mediante el comando `rcisdn start`. *Hotplug*, que se utiliza para dispositivos PCMCIA y USB, carga el controlador al enchufar el dispositivo. Cuando haya terminado con los ajustes, seleccione *Aceptar*.

En el siguiente cuadro de diálogo, especifique el tipo de interfaz de la tarjeta RDSI y añada ISP a una interfaz existente. Las interfaces pueden ser del tipo `SyncPPP` o `RawIP`, pero la mayoría de los ISP trabajan con el modo `SyncPPP`, que se describe a continuación.

Figura 18.6 *Configuración de la interfaz RDSI*



El número que hay que introducir en *Mi número de teléfono* depende de cada configuración concreta:

Tarjeta RDSI conectada directamente a la toma de teléfono
: Una línea RDSI estándar ofrece tres números de teléfono (los llamados números múltiples de suscriptor o MSN). Si el suscriptor pide más, pueden ser hasta 10. En este campo debe introducirse uno de estos MSN, pero sin el prefijo. Si se introduce un número incorrecto, el operador de telefonía volverá automáticamente al primer MSN asignado a la línea RDSI.

Tarjeta RDSI conectada a una centralita
: De nuevo, la configuración puede variar en función de los equipos instalados:

1. Las centralitas (PBX) pequeñas diseñadas para uso doméstico utilizan en su mayoría el protocolo Euro-ISDN (EDSS1) para las llamadas internas. Estas centralitas tienen un bus S0 interno y utilizan números internos para los equipos conectados a ellas.

   Utilice uno de los números internos como MSN. Debería poder utilizar al menos uno de los MSN de la centralita que se hayan habilitado para el marcado directo al exterior. Si no funciona, intente con un único cero. Para obtener más información, consulte la documentación de la centralita.

2. Las centralitas grandes diseñadas para empresas utilizan normalmente el protocolo 1TR6 para las llamadas internas. Su MSN se llama EAZ y normalmente corresponde al número de marcación directa. Para la configuración en Linux, debería ser suficiente introducir el último número del EAZ. Como último recurso, vaya intentando con los dígitos del 1 al 9.

Para que la conexión finalice justo antes de que se cargue la siguiente unidad de pago, habilite *ChargeHUP* (ChargeHUP). No obstante, recuerde que quizá no funcione con todos los ISP. También puede habilitar la unión de canales (multilink PPP) seleccionando la opción correspondiente. Finalmente, puede habilitar SuSEfirewall2 para el enlace seleccionando *Interfaz externa del cortafuegos* y *Reiniciar cortafuegos*. Para permitir que el usuario normal sin permisos de administrador active y desactive la interfaz, seleccione *Controlado por el usuario*.

Detalles abre un cuadro de diálogo en el que se pueden implementar esquemas de conexión más complejos, que no son importantes para usos domésticos. Salga del cuadro de diálogo *Detalles* seleccionando *Aceptar*.

En el siguiente cuadro de diálogo, realice los ajustes de la dirección IP. Si el proveedor no ha suministrado una dirección IP estática, seleccione *Dirección IP dinámica*. De lo contrario, utilice los campos que aparecen para introducir la dirección IP del host local

y la dirección IP remota, de acuerdo con las indicaciones del ISP. Si la interfaz debe ser la vía a Internet por defecto, seleccione *Ruta predeterminada*. Cada host sólo puede tener una interfaz configurada como vía por defecto. Salga del cuadro de diálogo seleccionando *Siguiente*.

El siguiente cuadro de diálogo permite establecer el país y seleccionar un ISP. Los ISP incluidos en la lista son sólo proveedores que ofrecen servicios de cobro por llamada. Si su ISP no se encuentra en la lista, seleccione *Nuevo*. Se abrirá el cuadro de diálogo *Parámetros del proveedor* en el que se introducen los datos del ISP. Al introducir el número de teléfono, no incluya espacios ni comas entre los dígitos. Para terminar, introduzca el nombre de usuario y la contraseña proporcionados por el ISP. Cuando acabe, seleccione *Siguiente*.

Para utilizar *Llamada bajo demanda* en una estación de trabajo individua, especifique también el servidor de nombres (servidor DNS). La mayoría de los ISP admiten DNS dinámico, lo que significa que el ISP envía la dirección IP del servidor de nombres cada vez que se realiza la conexión. Para una estación de trabajo individual, sin embargo, sigue siendo necesario introducir una dirección cualquiera, por ejemplo `192.168.22.99`. Si el ISP no admite DNS dinámico, especifique las direcciones IP de los servidores de nombres del ISP. Si lo desea, especifique un tiempo límite para la conexión (el periodo de inactividad de la red (en segundos) tras el cual la conexión finalizará automáticamente). Confirme sus ajustes con *Siguiente*. YaST mostrará un resumen de las interfaces configuradas. Para activar todos los ajustes, seleccione *Finalizar*.

18.4.4 Módem de cable

En algunos países, como Austria o los Estados Unidos, es muy común acceder a Internet por medio de la red de televisión por cable. El suscriptor de la televisión por cable recibe normalmente un módem que se conecta a la toma de salida del cable de televisión por un extremo y a la tarjeta de red del ordenador por el otro (mediante un par de cobre trenzado 10Base-TG). El módem de cable proporciona entonces una conexión dedicada a Internet con una dirección Ip fija.

En función de las instrucciones que proporcionadas por el ISP, seleccione *Automatic Address Setup (via DHCP)* (Configuración automática de direcciones (mediante DHCP)) o bien *Configuración de la dirección estática* cuando configure la tarjeta de red. Hoy en día, la mayoría de los proveedores utilizan DHCP. La dirección IP fija suele formar parte de una suscripción especial para empresas.

18.4.5 DSL

Para configurar un dispositivo DSL, seleccione el módulo *ADSL* de la sección *Dispositivos de red* de YaST. Este módulo de YaST se compone de varios cuadros de diálogo en los que se establecen los parámetros de los enlaces DSL basados en uno de los siguientes protocolos:

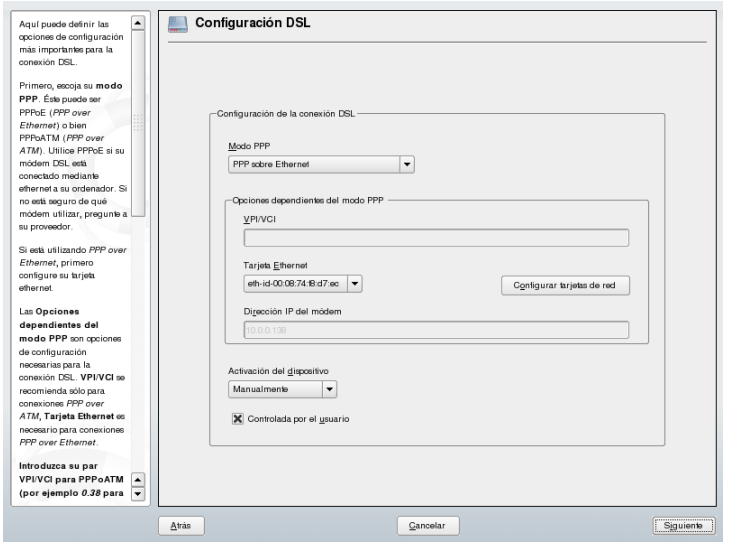
- PPP over Ethernet (PPPoE)
- PPP over ATM (PPPoATM)
- CAPI for ADSL (Fritz Cards)
- Point-to-Point Tunneling Protocol (PPTP) (Austria)

Para la configuración de una conexión DSL basada en PPPoE o PPTP es necesario que la tarjeta de red correspondiente ya esté correctamente configurada. Si aún no lo ha hecho, configure en primer lugar la tarjeta seleccionando *Configurar tarjetas de red* (consulte la Sección 18.4.1, “Configuración de la tarjeta de red de con YaST” (p. 363)). En el caso de los enlaces DSL, las direcciones pueden asignarse automáticamente, pero no mediante DHCP, por lo que no debe habilitarse la opción *Automatic address setup (via DHCP)* (Configuración automática de direcciones (mediante DHCP)). En lugar de ello, introduzca una dirección estática cualquiera, por ejemplo `192.168.22.1`. En *Máscara de subred*, introduzca `255.255.255.0`. Si está configurando una estación de trabajo individual, deje vacío *Pasarela predeterminada*.

SUGERENCIA

Los valores de *Dirección IP* y *Máscara de subred* son sólo de relleno. Sólo son necesarios para inicializar la tarjeta de red y no representan el enlace DSL como tal.

Figura 18.7 *Configuración DSL*



Para comenzar la configuración DSL (consulte la Figura 18.7, “Configuración DSL” (p. 373)), seleccione en primer lugar el modo PPP y la tarjeta ethernet a la que está conectado el módem DSL (en la mayoría de los casos, se trata de `eth0`). A continuación, utilice *Activación del dispositivo* para especificar si el enlace DSL debe establecerse durante el proceso de arranque. Haga clic en *Controlado por el usuario* para autorizar al usuario normal sin permisos de usuario root a que active y desactive la interfaz mediante KInternet. El cuadro de diálogo también permite seleccionar el país y elegir entre muchos de los ISP que operan en él. Los detalles de los siguientes cuadros de diálogo para la configuración DSL dependen de las opciones establecidas hasta el momento, por lo que sólo se mencionarán brevemente en los próximos párrafos. Para obtener más detalles acerca de las opciones disponibles, consulte la ayuda de los propios cuadros de diálogo.

Para utilizar *Llamada bajo demanda* en una estación de trabajo individua, especifique también el servidor de nombres (servidor DNS). La mayoría de los ISP admiten DNS dinámico (el ISP envía la dirección IP del servidor de nombres cada vez que se realiza la conexión). Para una estación de trabajo individual, sin embargo, sigue siendo necesario introducir una dirección cualquiera, por ejemplo `192.168.22.99`. Si el ISP no admite DNS dinámico, introduzca la dirección IP del servidor de nombres proporcionada por el ISP.

Tiempo de inactividad (en segundos) define el periodo de inactividad de la red tras la conexión se terminará automáticamente. Un valor razonable para el tiempo límite razonable es de entre 60 y 300 segundos. Si se inhabilita *Llamada bajo demanda*, puede ser útil establecer el valor del tiempo límite en cero para evitar que se cuelgue automáticamente.

La configuración de T-DSL es muy similar a la de DSL. Simplemente seleccione *T-Online* como proveedor y YaST abrirá el cuadro de diálogo de configuración de T-DSL. En este cuadro de diálogo, introduzca la información adicional necesaria para T-DSL (el ID de la línea, el número de T-Online, el código de usuario y la contraseña). Todo ello debería aparecer en la información que recibió al contratar T-DSL.

18.5 Gestión de conexiones de red con NetworkManager

NetworkManager constituye la solución ideal para las estaciones de trabajo móviles, ya que permite olvidarse de la configuración de interfaces de red y cambiar de una red a otra cuando cambie de ubicación. NetworkManager puede conectar automáticamente con las redes WLAN conocidas y, en el caso de que haya dos o más posibilidades de conexión, utilizar la más rápida.

NOTA: NetworkManager y SCPM

No se debe utilizar NetworkManager con SCPM cuando los perfiles SCPM impliquen también el cambio de los ajustes de red. Si quiere utilizar SCPM y NetworkManager al mismo tiempo, inhabilite los recursos de red en la configuración de SCPM.

No conviene utilizar NetworkManager en los casos siguientes:

- El equipo dispone de una dirección estática.
- Quiere utilizar más de un proveedor de acceso telefónico con una sola interfaz.
- Desea utilizar el cifrado WPA-EAP en la conexión WLAN.
- El equipo hace las funciones de router en la red.

- El equipo proporciona servicios de red a otros equipos de la red. Es, por ejemplo, un servidor DHCP o DNS.

18.5.1 Control de NetworkManager

Para iniciar NetworkManager, habilite NetworkManager en el módulo YaST del dispositivo de red. Debido a que NetworkManager no requiere una configuración de red estándar, la configuración de YaST pasa a estar inactiva. NetworkManager seleccionará automáticamente la mejor red disponible, aunque sólo podrá conectarse automáticamente a una red conocida. Para conectar con una red por primera vez, utilice el applet de NetworkManager. Si la red exige información adicional, como el nombre de usuario, la contraseña o la clave de cifrado, NetworkManager la solicitará.

KDE y GNOME tienen applets propios para NetworkManager. El applet adecuado debe iniciarse automáticamente con el entorno de escritorio. El applet aparece en forma de icono en la bandeja del sistema. Las funciones de ambos applets son similares, pero las interfaces son diferentes. También se pueden utilizar en otros entornos gráficos compatibles con la bandeja estándar del sistema.

Applet KNetworkManager

KNetworkManager es un applet diseñado para KDE que permite controlar NetworkManager. Si no se está ejecutando, inícielo con el comando `knetworkmanager`. Cuando se está ejecutando, en la bandeja del sistema aparece un icono que representa a la Tierra en azul. Al hacer clic con el botón derecho en el icono, se abre el menú de KNetworkManager con varios comandos para gestionar las conexiones de red.

El menú incluye las conexiones de red disponibles para los dispositivos fijos e inalámbricos. Si sitúa el cursor del ratón sobre ellos, aparecerán los detalles correspondientes. La conexión utilizada en cada momento se marcará en el menú. El menú también muestra la intensidad de la señal de las redes inalámbricas. Las redes inalámbricas cifradas se marcan con un icono de cerrojo azul. Para conectarse a una red cifrada, selecciónela en el menú. En el cuadro de diálogo que se abrirá, seleccione el tipo de *Cifrado* que utiliza la red e introduzca los datos adecuados en los campos *Frase de contraseña* y *Clave.*

Para conectarse a una red que no difunda su identificador de conjunto de servicios (ESSID), y por lo tanto no pueda detectarse automáticamente, seleccione *Conectar a*

otra red inalámbrica. En el cuadro de diálogo que se abrirá, introduzca el valor ESSID y defina los parámetros de cifrado si es necesario.

Para acceder a las conexiones de acceso telefónico, seleccione *Conexiones de acceso telefónico.* Si las conexiones de acceso telefónico ya están definidas, inicie la conexión haciendo clic en la que desee utilizar. *Configurar conexiones de acceso telefónico* abre YaST, lo que permite definir nuevas conexiones de acceso telefónico.

Para inhabilitar cualquier conexión de red activa, seleccione *Opciones → Cambiar al modo sin conexión.* en el menú de KNetworkManager. Para volver a habilitar la conexión, seleccione *Opciones → Cambiar al modo en línea.* Para inhabilitar las conexiones de red inalámbricas, seleccione *Opciones → Inhabilitar conexión inalámbrica* en el menú de KNetworkManager. Para volver a habilitar las conexiones inalámbricas, seleccione *Opciones → Habilitar conexión inalámbrica.* El sistema tardará unos segundos en habilitar la red.

Applet de NetworkManager para GNOME

GNOME también dispone de su propio applet para NetworkManager. Si no se está ejecutando, inícielo con el comando `nm-applet`. Cuando se está ejecutando, en la bandeja del sistema aparece un icono. El aspecto del icono depende del estado de la conexión de red. Si no está seguro de lo que significa el icono, sitúe el cursor del ratón sobre él hasta que aparezca una explicación.

Haga clic con el botón izquierdo en el icono del applet para que aparezca un menú con las redes disponibles. La conexión utilizada en cada momento se marcará en el menú. El menú también muestra la intensidad de la señal de las redes inalámbricas. Las redes inalámbricas cifradas se marcan con un icono de escudo. Para conectarse a una red cifrada, selecciónela en el menú. En el cuadro de diálogo que se abrirá, seleccione el tipo de *Cifrado* que utiliza la red e introduzca los datos adecuados en los campos *Frase de contraseña* y *Clave.*

Para conectarse a una red que no difunda su identificador de conjunto de servicios (ESSID), y por lo tanto no pueda detectarse automáticamente, haga clic con el botón izquierdo en el icono y seleccione *Conectar a otra red inalámbrica.* En el cuadro de diálogo que se abrirá, introduzca el valor ESSID y defina los parámetros de cifrado si es necesario.

Para inhabilitar la red, haga clic con el botón derecho en el icono del applet y desactive *Habilitar red.* Para inhabilitar la red inalámbrica, haga clic con el botón derecho en el icono del applet y desactive *Habilitar conexión inalámbrica.*

Para obtener información acerca de la conexión utilizada en cada momento (incluida la interfaz utilizada, la dirección IP y la dirección de hardware), haga clic con el botón derecho en el icono del applet y seleccione *Información de conexión* en el menú.

18.5.2 Información adicional

Para obtener más información acerca de NetworkManager y D-BUS, consulte los sitios Web y directorios siguientes:

- `http://www.gnome.org/projects/NetworkManager/`: página del proyecto NetworkManager
- `http://www.freedesktop.org/Software/dbus`: página del proyecto D-BUS
- `/usr/share/doc/packages/NetworkManager`

18.6 Configuración manual de una conexión de red

La configuración manual del software de red siempre debe ser la última alternativa. Se recomienda utilizar YaST. Sin embargo, la información básica acerca de la configuración de red también puede serle útil cuando trabaje con YaST.

Todas las tarjetas de red y de red hotplug integradas (PCMCIA, USB y algunas tarjetas PCI) se detectan y se configuran mediante hotplug. El sistema detecta una tarjeta de red de dos maneras: primero como un dispositivo físico y, después, como una interfaz. La inserción o detección de un dispositivo activa un evento hotplug. Este evento hotplug activa la inicialización del dispositivo mediante el guión `hwup`. Cuando la tarjeta de red se inicializa como una nueva interfaz de red, el núcleo genera otro evento hotplug que origina la configuración de la interfaz mediante `ifup`.

El núcleo numera los nombres de la interfaz en función del orden temporal del registro. La secuencia de inicialización es fundamental para la asignación de nombres. Si falla una de las tarjetas, se modificará la numeración de todas las que se inicien después. Para tarjetas hotplug reales, lo que importa es el orden en el que se conectan los dispositivos.

Para llevar a cabo una configuración flexible, la configuración del dispositivo (hardware) y de la interfaz debe realizarse por separado y la asignación de configuraciones a los dispositivos e interfaces no se gestiona mediante los nombres de interfaz. Las configuraciones del dispositivo se ubican en `/etc/sysconfig/hardware/hwcfg-*`. Las configuraciones de la interfaz se ubican en `/etc/sysconfig/network/ifcfg-*`. Los nombres de las configuraciones se asignan de modo que describan los dispositivos e interfaces a los que están asociados. Puesto que la primera asignación de controladores al nombre de la interfaz requería nombres de interfaz estáticos, esta asignación ya no se realizará en `/etc/modprobe.conf`. En el nuevo concepto, las entradas de alias en este archivo pueden causar efectos secundarios no deseados.

Los nombres de configuración, es decir, todo lo que aparece después de `hwcfg-` o de `ifcfg-`, pueden describir los dispositivos mediante la ranura, el ID específico del dispositivo o el nombre de la interfaz. Por ejemplo, el nombre de configuración para una tarjeta PCI puede ser `bus-pci-0000:02:01.0` (ranura PCI) o `vpid-0x8086-0x1014-0x0549` (ID del producto o del proveedor). El nombre de la interfaz asociada puede ser `bus-pci-0000:02:01.0` o `wlan-id-00:05:4e:42:31:7a` (dirección MAC).

Para asignar una configuración de red específica a una tarjeta de un tipo determinado (o del que sólo se ha insertado uno) en lugar de una tarjeta determinada, seleccione un número menor de nombres de configuración específicos. Por ejemplo, `bus-pcmcia` se utilizará para todas las tarjetas PCMCIA. Por otro lado, los nombres pueden estar limitados por un tipo de interfaz precedente. Por ejemplo, `wlan-bus-usb` se asignará a las tarjetas WLAN conectadas a un puerto USB.

El sistema siempre utiliza la configuración que mejor describa una interfaz o el dispositivo que suministre la interfaz. La búsqueda de la configuración más adecuada se gestiona mediante `getcfg`. La salida de `getcfg` proporciona toda la información que se puede utilizar para describir un dispositivo. Los detalles acerca de la especificación de los nombres de configuración están disponibles en la página del manual de `getcfg`.

Con el método descrito, una interfaz de red se establece con la configuración correcta incluso si los dispositivos de red no siempre se inicializan en el mismo orden. Sin embargo, el nombre de la interfaz sigue dependiendo de la secuencia de inicialización. Existen dos maneras de garantizar un acceso fiable a la interfaz de una determinada tarjeta de red:

- `getcfg-interface` *`nombre de configuración`* devuelve el nombre a la interfaz de red asociada. Sin embargo, el nombre de configuración, como por ejemplo cortafuegos, dhcpd, encaminamiento o varias interfaces de red virtuales (túneles), se puede introducir en algunos archivos de configuración en lugar del nombre de la interfaz, que no es permanente.

- Los nombres permanentes se asignan a cada interfaz automáticamente. Puede modificarlos para que se ajusten a sus necesidades. Cuando cree nombres de interfaz, proceda como se describe en `/etc/udev/rules.d/30-net_persistent_names.rules`. Sin embargo, el nombre permanente *`pname`* no debe ser el mismo que el nombre que el núcleo asignará automáticamente. Sin embargo, nombres como `eth*`, `tr*`, `wlan*` no están permitidos. En su lugar, utilice `net*` o nombres descriptivos como `externo`, `interno` o `dmz`. Asegúrese de que no se usa dos veces el mismo nombre de interfaz. Los caracteres permitidos están limitados a `[a-zA-Z0-9]`. Un nombre permanente sólo se puede asignar a una interfaz inmediatamente después de su registro, lo que quiere decir que el controlador de la tarjeta de red debe volver a cargarse o que `hwup` *`descripción de dispositivo`* debe ejecutarse. El comando `rcnetwork restart` (reiniciar) es insuficiente para este propósito.

IMPORTANTE: Uso de nombres de interfaces permanentes

El uso de nombres de interfaces permanentes se ha comprobado en todas las áreas. Sin embargo, puede que algunas aplicaciones no puedan gestionar nombres de interfaces seleccionados libremente.

`ifup` requiere que exista la interfaz, puesto que no inicializa el hardware. La inicialización del hardware se gestiona mediante el comando `hwup` (ejecutado por `hotplug` o `coldplug`). Cuando se inicializa un nuevo dispositivo, `ifup` se ejecuta de forma automática para la nueva interfaz mediante `hotplug` y la interfaz se configura si el modo de inicio es `onboot`, `hotplug` o `auto` y si se ha iniciado el servicio de `red`. Anteriormente, el comando `ifup` *`nombre de interfaz`* activaba la inicialización del hardware. Ahora, el procedimiento se ha invertido. Primero, se inicializa un componente de hardware y, a continuación, lo hacen el resto de aplicaciones. De este

modo, siempre se puede configurar un número variable de dispositivos de la mejor manera posible mediante un conjunto de configuraciones existentes.

La Tabla 18.5, "Guiones de configuración manual de red" (p. 380) resume los guiones más importantes implicados en la configuración de red. Cuando sea posible, los guiones se distinguen por el hardware y la interfaz.

Tabla 18.5 *Guiones de configuración manual de red*

Fase de configuración	Comando	Función
Hardware	`hw{up,down,status}`	El subsistema hotplug ejecuta los guiones `hw*` para inicializar un dispositivo, deshacer la inicialización o consultar el estado de un dispositivo. Existe más información disponible en la página del manual de `hwup`.
Interfaz	`getcfg`	`getcfg` se puede utilizar para consultar el nombre de la interfaz asociado a un nombre de configuración o a una descripción de hardware. Existe más información disponible en la página del manual de `getcfg`.
Interfaz	`if{up,down,status}`	Los guiones `if*` inician las interfaces de red existentes o vuelven al estado de la interfaz especificada. Existe más información disponible en la página del manual de `hwup`.

Para obtener información adicional acerca de hotplug y de los nombres de dispositivo permanentes, consulte el Capítulo 12, *Gestión dinámica de dispositivos de núcleo con udev* (p. 273).

18.6.1 Archivos de configuración

Esta sección proporciona una descripción general de los archivos de configuración de red, así como su propósito y el formato utilizado.

/etc/syconfig/hardware/hwcfg-*

Estos archivos contienen las configuraciones de hardware de las tarjetas de red y de otros dispositivos. Asimismo, también contienen los parámetros necesarios, como el módulo del núcleo, el modo de inicio y las asociaciones de guiones. Para obtener más detalles, consulte la página del manual de `hwup`. Independientemente del hardware existente, las configuraciones `hwcfg-static-*` se aplican cuando se inicia coldplug.

/etc/sysconfig/network/ifcfg-*

Estos archivos contienen las configuraciones para la interfaz de red. Incluyen información como el modo de inicio y la dirección IP. Los posibles parámetros se describen en la página del manual de `ifup`. Además, si se tiene que utilizar una configuración general para una única interfaz, todas las variables de los archivos `dhcp`, `wireless` y `config` se pueden utilizar en los archivos `ifcfg-*`.

/etc/sysconfig/network/config, dhcp, wireless

El archivo `config` contiene la configuración general para el comportamiento de `ifup`, `ifdown` e `ifstatus`. `dhcp` contiene la configuración de DHCP y `wireless` para las tarjetas LAN inalámbricas. Las variables de los tres archivos de configuración se describen y se pueden utilizar en los archivos `ifcfg-*`, cuando disponen de la máxima prioridad.

/etc/sysconfig/network/routes,ifroute-*

Aquí se determina el encaminamiento estático de los paquetes TCP/IP. Todas las rutas estáticas requeridas por las diferentes tareas del sistema se pueden introducir en el archivo `/etc/sysconfig/network/routes`: rutas al host, rutas al host mediante gateway y rutas a una red. Para cada interfaz que necesite una ruta individual, defina un archivo de configuración adicional: `/etc/sysconfig/network/ifroute-*`.

Sustituya * con el nombre de la interfaz. Las entradas de los archivos de configuración del encaminamiento se presentan de la manera siguiente:

```
# Destination     Dummy/Gateway     Netmask            Device
#
127.0.0.0         0.0.0.0           255.255.255.0      lo
204.127.235.0     0.0.0.0           255.255.255.0      eth0
default           204.127.235.41    0.0.0.0            eth0
207.68.156.51     207.68.145.45     255.255.255.255    eth1
192.168.0.0       207.68.156.51     255.255.0.0        eth1
```

El destino de la ruta se encuentra en la primera columna. Esta columna puede contener la dirección IP de red o host o, en el caso de servidores de nombre *accesibles*, la red o nombre de host completo.

La segunda columna contiene un gateway por defecto a través del cual se puede acceder a un host o a una red. La tercera columna contiene la máscara de red de redes o hosts tras un gateway. Por ejemplo, la máscara es `255.255.255.255` para un host tras un gateway.

La cuarta columna sólo es relevante para redes conectadas al host local como loopback, Ethernet, RDSI, PPP y dispositivo fantasma. Aquí se debe introducir el nombre del dispositivo.

Se puede utilizar una quinta columna optativa para especificar el tipo de ruta. Las columnas que no se necesiten deben incluir un signo menos `-` para que el analizador interprete correctamente el comando. Para obtener más detalles, consulte la página Man de `routes(5)`.

/etc/resolv.conf

En este archivo se especifica el dominio al que pertenece el host (contraseña `search` [buscar]). También se enumera el estado de la dirección del servidor de nombre al que se desea acceder (contraseña `nameserver` [servidor de nombre]). Se pueden especificar varios nombres de dominio. Al resolver un nombre incompleto, se realiza un intento de generar uno agregando entradas `search` (buscar) individuales. Utilice varios servidores de nombre introduciendo varias líneas, cada una de las cuales debe comenzar por `nameserver` (servidor de nombre). Anteponga signos # a los comentarios. YaST introduce el servidor de nombre especificado en este archivo. El Ejemplo 18.5, “`/etc/resolv.conf`” (p. 383) muestra la forma de `/etc/resolv.conf`.

Ejemplo 18.5 */etc/resolv.conf*

```
# Our domain
search example.com
#
# We use sun (192.168.0.20) as nameserver
nameserver 192.168.0.20
```

Algunos servicios, como `pppd` (`wvdial`), `ipppd` (`isdn`), `dhcp` (`dhcpcd` y `dhclient`), `pcmcia` y `hotplug` modifican el archivo `/etc/resolv.conf` mediante el guión `modify_resolvconf`. Si el archivo `/etc/resolv.conf` se ha modificado de forma temporal mediante este guión, entonces incluirá un comentario predefinido que proporciona información acerca del servicio que lo modifica, la ubicación en la que se ha realizado la copia de seguridad del archivo original y el modo de desactivar el mecanismo de modificación automático. Si `/etc/resolv.conf` se modifica varias veces, el archivo incluirá modificaciones en un formulario anidado. Estas modificaciones se pueden invertir incluso si el orden de la inversión es diferente del orden de la introducción de las modificaciones. Los servicios que incluyen esta flexibilidad incluyen `isdn`, `pcmcia` y `hotplug`.

Si no se ha terminado un servicio de forma normal y limpia, `modify_resolvconf` se puede utilizar para restaurar el archivo original. Incluso durante el arranque del sistema, se realiza una comprobación para localizar un `resolv.conf` sin limpiar y modificado, por ejemplo, después de un fallo del sistema, en cuyo caso se restaurará el `resolv.conf` original (sin modificar).

YaST utiliza el comando `modify_resolvconf check` para saber si `resolv.conf` se ha modificado y, a continuación, advierte al usuario de que se perderán los cambios después de restaurar el archivo. Además de esto, YaST no se basa en `modify_resolvconf`, lo que significa que el impacto del cambio de `resolv.conf` mediante YaST es el mismo que para cualquier cambio manual. En ambos casos, el efecto de los cambios es permanente. Las modificaciones solicitadas por los servicios mencionados son sólo temporales.

`/etc/hosts`

En este archivo, que se muestra en el Ejemplo 18.6, “`/etc/hosts`” (p. 384), las direcciones IP están asignadas a nombres de host. Si no se implementa ningún servidor de nombre, deberá aparecer una lista de todos los hosts para los que se va a configurar una conexión IP. Para cada host, introduzca una línea que conste de la dirección IP, del nombre de host completo y del nombre de host en el archivo. La dirección IP debe

ubicarse al principio de la línea y las entradas deben estar separadas por espacios y pestañas. Los comentarios siempre van precedidos de #.

Ejemplo 18.6 */etc/hosts*

```
127.0.0.1 localhost
192.168.0.20 sun.example.com sun
192.168.0.0 earth.example.com earth
```

/etc/networks

Aquí, los nombres de red se convierten en direcciones de red. El formato es similar al del archivo `hosts`, excepto que los nombres de red van situados delante de la dirección. Consulte el Ejemplo 18.7, "`/etc/networks`" (p. 384).

Ejemplo 18.7 */etc/networks*

```
loopback     127.0.0.0
localnet     192.168.0.0
```

/etc/host.conf

La resolución de nombres, es decir, la traducción de los nombres de red y de host mediante la biblioteca *resolver* está controlada por este archivo. Este archivo sólo se utiliza para programas relacionados con libc4 o libc5. Para los programas glibc en curso, consulte la configuración de `/etc/nsswitch.conf`. Siempre debe haber un único parámetro en su propia línea. Los comentarios van precedidos de #. La Tabla 18.6, "Parámetros para /etc/host.conf" (p. 384) muestra los parámetros disponibles. En Ejemplo 18.8, "`/etc/host.conf`" (p. 385) se muestra el ejemplo de `/etc/host.conf`.

Tabla 18.6 *Parámetros para /etc/host.conf*

order *hosts*, *bind*	Especifica el orden de acceso a los servicios para la resolución de nombre. Los argumentos disponibles son (separados por espacios y comas) los siguientes: *hosts*: Busca el archivo `/etc/hosts` *bind*: Accede a un servidor de nombre

	nis: Utiliza NIS
multi *on*/*off*	Define si un host introducido en `/etc/hosts` puede tener varias direcciones IP.
nospoof *on* spoofalert *on*/*off*	Estos parámetros determinan el servidor de nombre *spoofing*, pero no la configuración de red.
trim *domainname*	El nombre del dominio especificado se separa del nombre de host después de la resolución de nombres de host (siempre que el nombre de host incluya el nombre del dominio). Esta opción resulta útil sólo si los nombres del dominio local se incluyen en el archivo `/etc/hosts`, pero deben seguir reconociéndose con los nombres del dominio adjunto.

Ejemplo 18.8 */etc/host.conf*

```
# We have named running
order hosts bind
# Allow multiple addrs
multi on
```

/etc/nsswitch.conf

La introducción a GNU C Library 2.0 va acompañada de la introducción de *Conmutador de servicio de nombre* (NSS). Para obtener más información, consulte la página Man de `nsswitch.conf(5)` y *GNU C Library Reference Manual* (Manual de referencia de la biblioteca GNU C).

El orden de las consultas se define en el archivo `/etc/nsswitch.conf`. En el Ejemplo 18.9, "`/etc/nsswitch.conf`" (p. 386) se muestra un ejemplo de `nsswitch.conf`. Los comentarios van precedidos de #. En este ejemplo, cuando se introduce un elemento en la base de datos `hosts`, se envía una petición a `/etc/hosts` (`files`) mediante DNS (consulte el Capítulo 20, *Sistema de nombres de dominio (DNS)* (p. 397)).

Ejemplo 18.9 */etc/nsswitch.conf*

```
passwd:     compat
group:      compat

hosts:      files dns
networks:   files dns

services:   db files
protocols:  db files

netgroup:   files
automount:  files nis
```

Las "bases de datos" disponibles en NSS se enumeran en la Tabla 18.7, "Bases de datos disponibles mediante /etc/nsswitch.conf" (p. 386). Además, `automount`, `bootparams`, `netmasks` y `publickey` están previstas en un futuro próximo. Las opciones de configuración para las bases de datos NSS se enumeran en la Tabla 18.8, "Opciones de configuración para las "bases de datos" NSS" (p. 387).

Tabla 18.7 *Bases de datos disponibles mediante /etc/nsswitch.conf*

`aliases`	Alias de correo implementados por `sendmail`; consulte `man 5 aliases`.
`ethers`	Direcciones Ethernet.
`group`	Para grupos de usuarios, utilizado por `getgrent`. Consulte también la página Man de `group`.
`hosts`	Para nombres de host y direcciones IP, utilizado en `gethostbyname` y en funciones similares.
`netgroup`	Host válido y listas de usuarios en la red para controlar los permisos de acceso; consulte la página Man de `netgroup(5)`.
`redes`	Nombres y direcciones de red, utilizado por `getnetent`.
`passwd`	Contraseñas de usuario, utilizado en `getpwent`; consulte la página Man de `passwd(5)`.

`protocols`	Protocolos de red, utilizado en `getprotoent`; consulte la página Man de `protocols(5)`.
`rpc`	Nombres y direcciones de llamadas de procedimientos remotos, utilizado en `getrpcbyname` y en funciones similares.
`services`	Servicios de red, utilizados por `getservent`.
`shadow`	Contraseñas shadow de usuarios, utilizadas en `getspnam`; consulte la página Man de `shadow(5)`.

Tabla 18.8 *Opciones de configuración para las "bases de datos" NSS*

`files`	Archivos de acceso directo, por ejemplo, `/etc/aliases`
`db`	Acceso mediante la base de datos
`nis`, `nisplus`	NIS, consulte también el Capítulo 21, *Uso de NIS* (p. 421)
`dns`	Sólo se puede utilizar como una extensión para `hosts` y `networks`
`compat`	Sólo se puede utilizar como una extensión de `passwd`, `shadow` y `group`

`/etc/nscd.conf`

Este archivo se utiliza para configurar nscd (daemon NSC). Consulte las páginas Man de `nscd(8)` y `nscd.conf(5)`. Por defecto, nscd almacena en caché las entradas de sistema de `passwd` y `groups`. Esto es importante para el funcionamiento de los servicios del directorio, como NIS y LDAP, puesto que si no, se necesitará la conexión de red para cada acceso a los nombres o grupos. `hosts` no se almacena en caché por defecto, puesto que el mecanismo de nscd para almacenar los hosts en caché no posibilita que el sistema local certifique comprobaciones de búsqueda adelante y atrás. En lugar de solicitar que nscd almacene nombres en caché, configure un servidor DNS de almacenamiento en caché.

Si el almacenamiento en caché para `passwd` está activado, por general, transcurrirán quince segundos hasta que se reconozca un nuevo usuario local agregado. Reduzca este tiempo límite reiniciando nscd con el comando `rcnscd restart` (reiniciar).

/etc/HOSTNAME

Contiene el nombre de host sin el nombre de dominio adjunto. Varios guiones pueden leer este archivo mientras la máquina está arrancando. Puede contener una única línea en la que se establece el nombre de host.

18.6.2 Guiones de inicio

Además de los archivos de configuración descritos anteriormente, también existen varios guiones para cargar los programas de red durante el arranque de la máquina. Éstos se inician en cuanto el sistema cambia a uno de los *niveles de ejecución multiusuario*. Algunos de estos guiones se describen en la Tabla 18.9, “Guiones de inicio para programas de red” (p. 388).

Tabla 18.9 *Guiones de inicio para programas de red*

`/etc/init.d/network`	Este guión gestiona la configuración de las interfaces de red. El hardware ya se debe haberse inicializado con `/etc/init.d/coldplug` (mediante `hotplug`). Si el servicio `network` no se ha iniciado, no se implementarán interfaces de red cuando se inserten mediante hotplug.
`/etc/init.d/inetd`	Los inicios xinetd. xinetd se pueden utilizar para que los servicios del servidor estén disponibles en el sistema. Por ejemplo, puede iniciar vsftpd siempre que se inicie una conexión FTP.
`/etc/init.d/portmap`	Inicia el portmap necesario para el servidor RPC, como por ejemplo un servidor NFS.
`/etc/init.d/nfsserver`	Inicia el servidor NFS.

`/etc/init.d/sendmail`	Controla el proceso de envío de correo.
`/etc/init.d/ypserv`	Inicia el servidor NIS.
`/etc/init.d/ypbind`	Inicia el servidor NIS.

18.7 smpppd como asistente de acceso telefónico

La mayoría de los usuarios particulares no disponen de una línea específica de conexión a Internet. En su lugar, utilizan conexiones de acceso telefónico. En función del método de acceso telefónico (ISDN o DSL), la conexión estará controlada por ipppd ó pppd. Prácticamente, todo lo que se necesita hacer para obtener una conexión en línea es iniciar correctamente los programas.

Si dispone de una conexión de tarifa plana que no genera ningún coste adicional para la conexión de acceso telefónico, sólo tiene que iniciar el correspondiente daemon. Controle la conexión de acceso telefónico con un applet KDE o una interfaz de línea de comando. Si el gateway de Internet no es el host utilizado por el usuario, éste podrá controlar la conexión de acceso telefónico mediante un host de red.

Aquí es donde interviene smpppd. Proporciona una interfaz uniforme para programas auxiliares y funciona en dos direcciones. En primer lugar, programa el pppd ó ipppd requerido y controla sus propiedades de acceso telefónico. En segundo lugar, facilita varios proveedores a los programas de usuario y transmite información acerca del estado actual de la conexión. Como smpppd se puede controlar mediante una red, es adecuado para controlar las conexiones de acceso telefónico a Internet desde una estación de trabajo en una subred privada.

18.7.1 Configuración de smpppd

YaST configura automáticamente las conexiones proporcionadas por smpppd. Los programas de acceso telefónico KInternet y cinternet también están configurados

previamente. Sólo se requiere la configuración manual para configurar las funciones adicionales de smpppd, como por ejemplo, el control remoto.

El archivo de configuración de smpppd es `/etc/smpppd.conf`. Por defecto, no habilita el control remoto. Las opciones más importantes de este archivo de configuración son las siguientes:

open-inet-socket = *`yes|no`*
: Para controlar smpppd a través de la red, está opción debe establecerse en `yes`. El puerto en el que smpppd escucha es `3185`. Si este parámetro está establecido en `yes`, los parámetros `bind-address`, `host-range` y `password` deben estár establecidos según corresponda.

bind-address = *`ip`*
: Si un host tiene varias direcciones IP, utilice este parámetro para determinar en qué dirección IP smpppd debe aceptar conexiones.

host-range = *`min ip max ip`*
: El parámetro `host-range` define el rango de la red. Los hosts cuya dirección IP se encuentra en este rango tienen autorizado el acceso a smpppd. Todos los hosts que no se encuentren en este rango tienen el acceso denegado.

password = *`password`*
: La asignación de una contraseña, permite a los clientes acceder solo a los hosts autorizados. Como se trata de una contraseña de sólo texto, no debe sobrevalorar la seguridad que proporciona. Si no hay ninguna contraseña asignada, todos los clientes tienen permitido el acceso a smpppd.

slp-register = *`yes|no`*
: Con este parámetro, el servicio smpppd se anuncia en la red a través de SLP.

Existe más información disponible acerca de smpppd en las páginas Man de `smpppd(8)` y `smpppd.conf(5)`.

18.7.2 Configuración de KInternet, cinternet y qinternet para uso remoto

KInternet, cinternet y qinternet se pueden utilizar para controlar un smpppd local o remoto. cinternet es la línea de comando correspondiente para el KInternet gráfico.

qinternet es prácticamente igual que KInternet, pero no utiliza librerias KDE, por lo que se puede utilizar sin KDE y debe instalarse aparte. Para preparar estas utilidades para su uso con un smpppd remoto, edite manualmente el archivo de configuración `/etc/smpppd-c.conf` o utilice KInternet. Este archivo sólo utiliza tres opciones:

sites = *`list of sites`*
: Especifica a las interfaces donde deben buscar smpppd. Las interfaces prueban las opciones en el orden que se especifica a continuación. La opción `local` ordena el establecimiento de una conexión al smpppd local. `gateway` indica un smpppd en el gateway. La conexión debe establecerse tal y como se especifica en `server` en `config-file`. `slp` ordena a las interfaces que se conecten al smpppd encontrado a través de SLP.

server = *`server`*
: Especifique el host en el que se ejecuta smpppd.

password = *`password`*
: Introduzca la contraseña seleccionada para smpppd.

Si smpppd está activo, puede intentar acceder a él, por ejemplo, mediante `cinternet --verbose --interface-list`. Si tiene dificultades, consulte las páginas Man de `smpppd-c.conf(5)` y `cinternet(8)`.

19 Servicios SLP en la red

El *protocolo de ubicación de servicios* (SLP) se ha desarrollado para simplificar la configuración de los clientes de red en una red local. Para configurar un cliente de red, incluyendo todos los servicios requeridos, el administrador necesita un conocimiento detallado de los servidores disponibles en la red. SLP comunica la disponibilidad de los servicios seleccionados a todos los clientes de la red local. Las aplicaciones compatibles con SLP pueden utilizar la información distribuida y se pueden configurar de forma automática.

SUSE Linux es compatible con la instalación mediante fuentes de instalación proporcionadas por SLP y contiene muchos servicios de sistema con compatibilidad integrada para SLP. YaST y Konqueror contienen las interfaces adecuadas para SLP. Puede utilizar SLP para proporcionar a los clientes de red funciones centrales, como por ejemplo, servidores de instalación, servidores YOU, de archivos o de impresión en SUSE Linux.

19.1 Registro de sus propios servicios

Existen muchas aplicaciones que se ejecutan en SUSE Linux que ya disponen de compatibilidad para SLP integrada mediante la utilización de la librería `libslp`. Si un servicio no se ha compilado con la compatibilidad para SLP, utilice uno de los métodos siguientes para que esté disponible con SLP:

Registro estático mediante `/etc/slp.reg.d`
: Cree un archivo de registro separado para cada servicio nuevo. A continuación, se muestra un ejemplo de archivo para registrar un servicio de escáner:

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

La línea más importante de este archivo es *URL de servicio*, que comienza por `servicio:`. Contiene el tipo de servicio (`scanner.sane`) y la dirección para la que el servicio está disponible en el servidor. *`$HOSTNAME`* se reemplaza automáticamente con el nombre de host completo. Detrás de éste aparece, separado por una coma, el nombre del puerto TCP en el que se puede encontrar el servicio correspondiente. A continuación, introduzca el idioma del servicio y la duración del registro en segundos. Estos datos deben separase de la URL de servicio por comas. Establezca el valor de la duración del registro entre `0` y `65535`. `0` evita el registro. `65535` elimina todas las restricciones.

El archivo de registro incluye además las dos variables `watch-tcp-port` y `description`. `watch-tcp-port` enlaza el anuncio del servicio de SLP con el estado del servicio haciendo que slpd lo compruebe. La segunda variable contiene una descripción más precisa del servicio que aparece en los navegadores correspondientes.

Registro estático mediante `/etc/slp.reg`
: La única diferencia con el procedimiento de `/etc/slp.reg.d` reside en la agrupación de todos los servicios en un archivo central.

Registro dinámico mediante slptool
: Si un servicio debe registrarse en SLP desde guiones patentados, utilice la interfaz de línea de comando slptool.

19.2 Interfaces SLP en SUSE Linux

SUSE Linux contiene varias interfaces que habilitan información SLP para su selección y utilización mediante una red:

slptool
: slptool es un sencillo programa de la línea de comandos que se puede utilizar para anunciar búsquedas SLP en la red o servicios patentados. `slptool --help` muestra todas las opciones y funciones disponibles. También se puede llamar a slptool desde guiones que procesen información SLP.

Navegador SLP de YaST
: YaST contiene un navegador SLP independiente que muestra todos los servicios de la red local anunciados a través de SLP en un diagrama de árbol en *Servicios de red → Navegador SLP*.

Konqueror
: Si se utiliza como un navegador de red, Konqueror muestra todos los servicios SLP disponibles de la red local en `slp:/`. Haga clic en los iconos de la ventana principal para obtener información detallada acerca del servicio correspondiente. Si utiliza Konqueror con `service:/`, haga clic en el icono correspondiente de la ventana del navegador para configurar una conexión con el servicio seleccionado.

19.3 Activación de SLP

Debe ejecutar slpd en el sistema si desea ofrecer servicios. No es necesario iniciar el daemon sólo para realizar búsquedas de servicio. Como la mayoría de los servicios de SUSE Linux, el daemon slpd se controla mediante un guión init independiente. Por defecto, el daemon está inactivo. Si desea activarlo para la duración de una sesión, ejecute `rcslpd start` como usuario `Root` para iniciarlo y `rcslpd stop` para detenerlo. Reinicie el sistema o realice una comprobación del estado mediante `restart` o `status`. Si por defecto, slpd está activa, ejecute el comando `insserv slpd` una sola vez como `root`. Esto incluye automáticamente slpd en el conjunto de servicios que se inician cuando un sistema arranca.

19.4 Información adicional

Las siguientes fuentes proporcionan información adicional acerca de SLP:

RFC 2608, 2609, 2610
: RFC 2608 describe, de forma general, la definición de SLP. RFC 2609 describe detalladamente la sintaxis de la URL de servicio utilizada y RFC 2610 describe DHCP mediante SLP.

http://www.openslp.com
: Página principal del proyecto OpenSLP.

/usr/share/doc/packages/openslp
: Este directorio contiene toda la documentación disponible para SLP, además incluye un archivo `README (LÉAME).SuSE` que contiene los detalles de SUSE Linux, de los RFC mencionados anteriormente y dos documentos HTML introductorios. Los programadores que deseen utilizar las funciones SLP deben instalar el paquete `openslp-devel` para consultar la *Programmers Guide* (Guía de programadores) que se incluye.

Sistema de nombres de dominio (DNS) 20

El sistema de nombres de dominio (DNS) es necesario para transformar los nombres de dominio y los de host en direcciones IP. De esta forma, la dirección IP 192.168.0.0 está asignada al nombre de host `earth`, por ejemplo. Antes de configurar su propio servidor de nombres, lea la información general acerca de DNS en la Sección 18.3, "Resolución de nombres" (p. 361). Los siguientes ejemplos de configuración se refieren a BIND.

20.1 Terminología de DNS

Zona
: El espacio de nombres de dominio está dividido en regiones denominadas "zonas". Por ejemplo, si cuenta con opensuse.org, la sección o zona será `opensuse` y el dominio `org`.

Servidor DNS
: Se trata de un servidor que mantiene el nombre y la información de IP para un dominio. Puede tener un servidor DNS primario para la zona principal, un servidor secundario para la zona esclava o un servidor esclavo sin zonas para el almacenamiento en caché.

  Servidor DNS de la zona principal
  : La zona principal incluye todos los hosts de la red. La zona principal de un servidor DNS almacenará los registros actualizados para todos los hosts del dominio.

Servidor DNS de la zona esclava
: Una zona esclava es una copia de la zona principal. El servidor DNS de la zona esclava obtiene los datos de la zona mediante operaciones de transferencia de zona desde el servidor principal. El servidor DNS de la zona esclava responde de manera autorizada por la zona, siempre que tenga datos válidos de ésta (que no hayan caducado). Si el esclavo no puede obtener una copia nueva de los datos de la zona, deja de responder por la zona.

Remitente
: Los remitentes son servidores DNS a los que el servidor DNS debería enviar las consultas que no pueda responder.

Registro
: El registro es la información acerca del nombre y la dirección IP. Los registros admitidos y su sintaxis se describen en la documentación de BIND. Algunos registros especiales son:

  Registro NS
  : Un registro NS le indica a los servidores de nombres qué equipos están a cargo de una zona de dominio determinada.

  Registro MX
  : Los registros MX (intercambio de correo) describen los equipos con los que contactar para dirigir correo a través de Internet.

  Registro SOA
  : El registro SOA (Inicio de autoridad) es el primer registro de un archivo de zona. El registro SOA se emplea cuando se usa DNS para sincronizar datos entre varios equipos.

20.2 Configuración con YaST

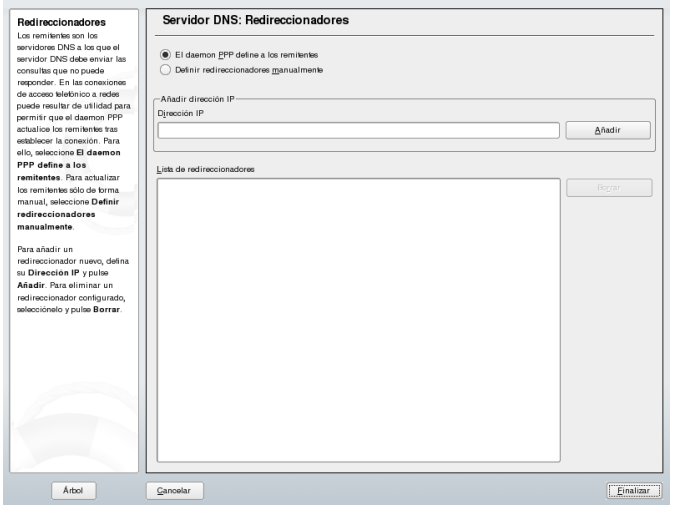
Puede usar el módulo DNS de YaST para configurar un servidor DNS para la red local. Al iniciar el módulo por primera vez, se iniciará un asistente en el que tendrá que tomar algunas decisiones básicas relativas a la administración del servidor. Cuando se completa esta configuración inicial se obtiene una configuración del servidor muy básica que debe de funcionar en los aspectos más esenciales. Se puede utilizar el modo avanzado para realizar tareas de configuración más precisas.

20.2.1 Configuración del asistente

El asistente consta de tres pasos o cuadros de diálogo. En los lugares específicos de los cuadros de diálogo, se le da la oportunidad de entrar en el modo de configuración avanzada.

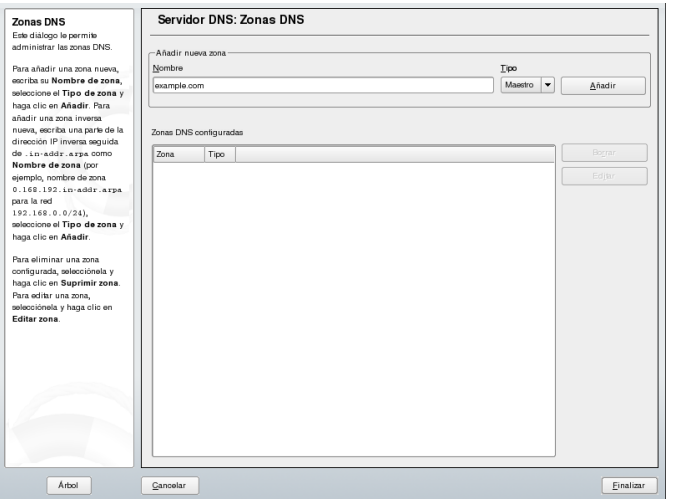
1 Al iniciar el módulo la primera vez, el cuadro de diálogo *Configuración del redireccionador,* que se muestra en la Figura 20.1, “Instalación del servidor DNS: Configuración del redireccionador” (p. 399), se abre. En él, decida si el daemon PPP debería ofrecer una lista de remitentes en una conexión de acceso telefónico mediante DSL o RDSI *(El daemon PPP define a los remitentes)* o si desea ofrecer su propia lista *(Definir redireccionadores manualmente).*

Figura 20.1 *Instalación del servidor DNS: Configuración del redireccionador*



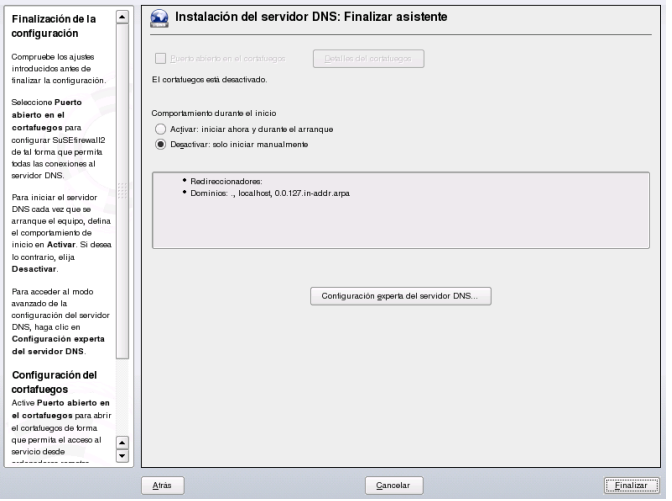
2 El cuadro de diálogo *Zonas DNS* tiene varias partes y es responsable de la gestión de archivos de zona, descritos en la Sección 20.5, “Archivos de zona” (p. 412). Para una nueva zona, escriba un nombre en *Nombre de zona.* Para añadir una zona inversa, el nombre debe terminar en `.in-addr.arpa`. Por último, seleccione *Tipo de zona* (principal o esclava). Consulte la Figura 20.2, “Instalación del servidor DNS: Zonas DNS” (p. 400). Haga clic en *Editar zona* para configurar otros ajustes de una zona existente. Para eliminar una zona, haga clic en *Suprimir zona.*

Figura 20.2 *Instalación del servidor DNS: Zonas DNS*



3 En el último cuadro de diálogo, puede abrir los puertos para el servicio DNS en el cortafuegos que se activa durante la instalación y decidir si DNS debería iniciarse. Desde este cuadro de diálogo se puede acceder a la configuración avanzada. Consulte la Figura 20.3, “Instalación del servidor DNS: Finalizar asistente” (p. 401).

Figura 20.3 *Instalación del servidor DNS: Finalizar asistente*



20.2.2 Configuración avanzada

Después de iniciar el módulo, YaST abre una ventana que muestra varias opciones de configuración. Al terminar la operación aparecerá la configuración del servidor DNS con las funciones básicas definidas:

Inicio del servidor DNS

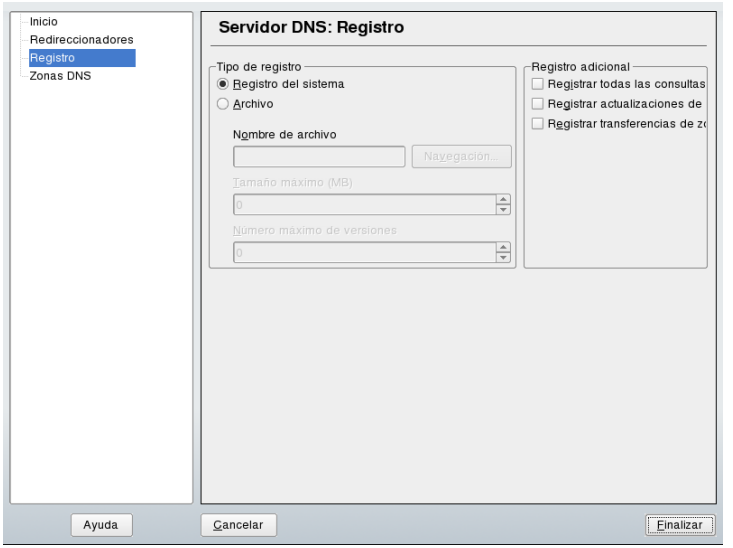
En *Arranque* defina si el servidor DNS debería iniciarse durante el arranque del sistema o manualmente. Para iniciar el servidor DNS inmediatamente, seleccione *Iniciar servidor DNS ahora.* Para detener el servidor DNS, seleccione *Detener servidor DNS ahora.* Para guardar los ajustes actuales, seleccione *Guardar la configuración y reiniciar el servidor DNS ahora.* Puede abrir el puerto DNS en el cortafuegos mediante la opción *Puerto abierto en el cortafuegos* y modificar los ajustes del cortafuegos con *Detalles del cortafuegos.*

Registro

Para definir lo que el servidor DNS debería registrar y cómo, seleccione *Registro.* En *Tipo de registro* especifique dónde debería escribir los datos de registro el servidor DNS. Utilice el archivo de registro de todo el sistema `/var/log/messages` seleccionando *Registrar al registro del sistema* o especifique un archivo diferente seleccionando *Registrar a archivo.* En el último caso, especifique además el tamaño máximo del archivo en megabytes y el número de archivos de registro que se van a almacenar.

Hay más opciones disponibles en *Registro adicional.* Al marcar la casilla *Registrar todas las consultas DNS* se obliga a que se registre *cada* consulta, por lo que el archivo de registro podría ser extremadamente grande. Por este motivo, no es buena idea marcarla para otras acciones que no sean de depuración. Para registrar el tráfico de datos durante las actualizaciones de zonas entre el servidor DHCP y DNS, marque *Registrar actualizaciones de zona.* Para registrar el tráfico de datos durante una transferencia de zona principal a esclava, marque *Registrar transferencias de zona.* Consulte la Figura 20.4, “Servidor DNS: Registro” (p. 402).

Figura 20.4 *Servidor DNS: Registro*

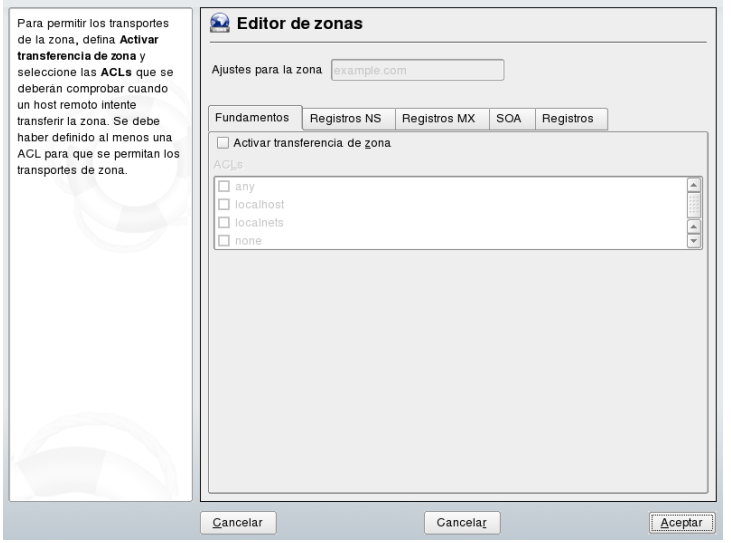


Cómo añadir una zona esclava

Para añadir una zona esclava, seleccione *Zonas DNS,* el tipo de zona *Esclava* y haga clic en *Añadir.*

En el *Editor de zonas,* en *IP del servidor DNS maestro,* especifique el servidor principal desde el que el esclavo debería recuperar sus datos. Para limitar el acceso al servidor, seleccione una de las ACL de la lista. Consulte la Figura 20.5, “Servidor DNS: editor de zonas esclavas” (p. 403).

Figura 20.5 *Servidor DNS: editor de zonas esclavas*



Cómo añadir una zona principal

Para añadir una zona principal, seleccione *Zonas DNS,* el tipo de zona *Maestra,* escriba el nombre de la zona nueva y haga clic en *Añadir.*

Cómo editar una zona principal

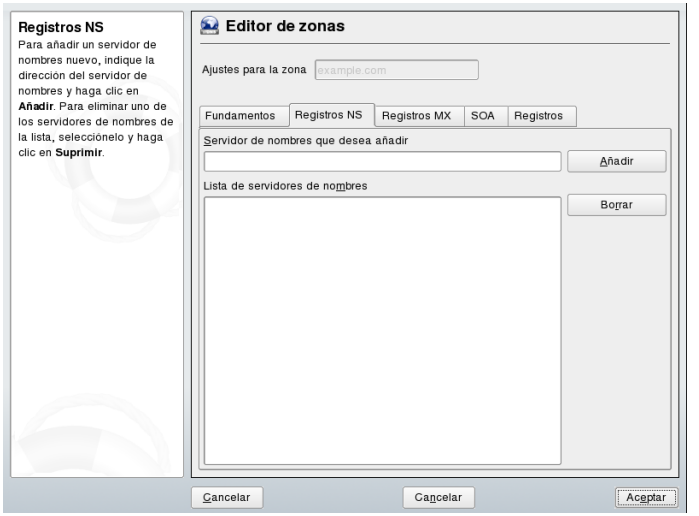
Para editar una zona principal, seleccione *Zonas DNS,* seleccione el tipo de zona *Maestra,* seleccione la zona principal de la tabla y haga clic en *Editar.* El cuadro de

diálogo está compuesto de varias páginas: *Fundamentos* (la primera que se abre), *Registros NS, Registros MX, SOA* y *Registros.*

Editor de zonas (registros NS)

Este cuadro de diálogo permite definir servidores de nombres alternativos para las zonas especificadas. Asegúrese de que su propio servidor de nombres está incluido en la lista. Para añadir un registro, escriba su nombre en *Servidor de nombres que desea añadir* y confirme a continuación haciendo clic en *Añadir.* Consulte la Figura 20.6, “Servidor DNS: Editor de zonas (registros NS)” (p. 404).

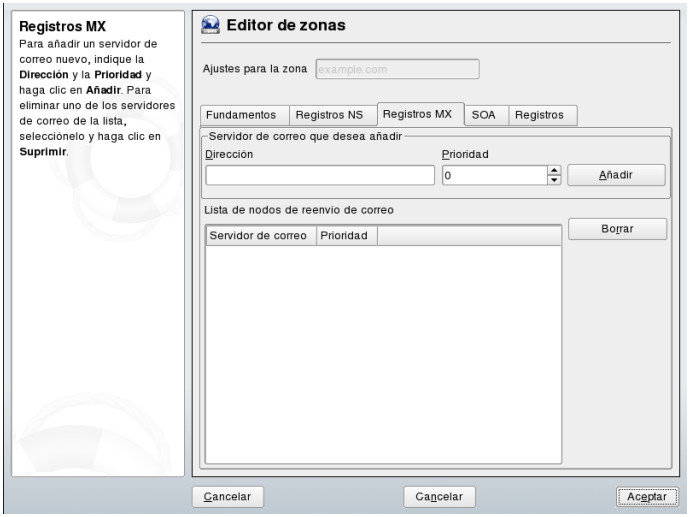
Figura 20.6 *Servidor DNS: Editor de zonas (registros NS)*



Editor de zonas (registros MX)

Para añadir a la lista existente un servidor de correo para la zona actual, escriba la dirección correspondiente y el valor de prioridad. Después de hacerlo, confirme seleccionando *Añadir.* Consulte la Figura 20.7, “Servidor DNS: Editor de zonas (registros MX)” (p. 405).

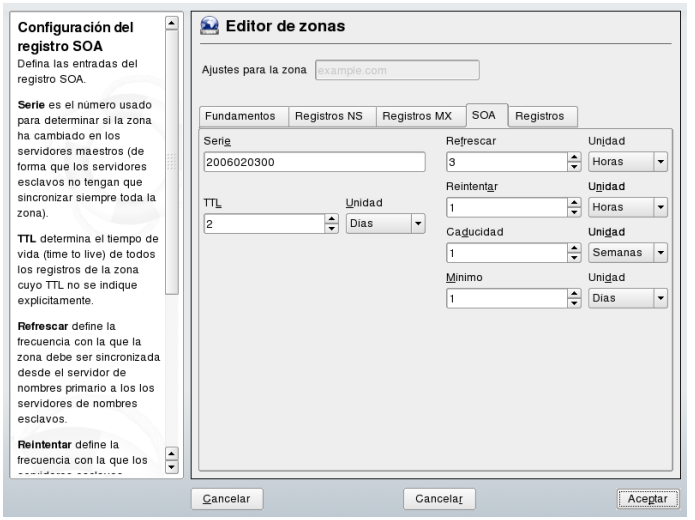
Figura 20.7 *Servidor DNS: Editor de zonas (registros MX)*



Editor de zonas (SOA)

Esta página le permite crear registros SOA (Inicio de autoridad). Para obtener una explicación de las opciones individuales, consulte el Ejemplo 20.6, “Archivo /var/lib/named/world.zone” (p. 413).

Figura 20.8 *Servidor DNS: Editor de zonas (SOA)*



Editor de zonas (registros)

Este cuadro de diálogo permite gestionar la resolución de nombres. En *Clave de registro* introduzca el nombre de host y a continuación seleccione el tipo. El registro A representa la entrada principal. El valor debería ser una dirección IP. *CNAME* es un alias. Utilice los tipos *NS* y *MX* para registros detallados o parciales que se añadan a la información de las pestañas *Registros NS* y *Registros MX.* Estos tres tipos se resuelven en un registro A existente. *PTR* es para zonas inversas. Es lo opuesto a un registro A.

20.3 Inicio del servidor de nombres BIND

En un sistema SUSE Linux, el servidor de nombres BIND *(Berkeley Internet Name Domain, Dominio de nombres de Internet de Berkeley)* viene configurado previamente, de manera que puede iniciarse justo después de la instalación sin ningún problema. Si ya hay una conexión de Internet y ha introducido `127.0.0.1` como la dirección del servidor de nombres para `localhost` en `/etc/resolv.conf`, por lo general ya tendrá una resolución de nombres en funcionamiento sin tener que saber el DNS del proveedor. BIND lleva a cabo una resolución de nombres mediante el servidor de nombres raíz, un proceso mucho más lento. Por norma general, debería introducirse el DNS del proveedor con su dirección IP en el archivo de configuración `/etc/named.conf` en la línea `forwarders` para asegurar una resolución de nombres efectiva y segura. Si todo esto funciona hasta ahora, el servidor de nombres se ejecutará como un servidor de nombres *sólo para almacenamiento en caché.* Únicamente cuando configure sus propias zonas, se convertirá en un DNS adecuado. En la documentación de `/usr/share/doc/packages/bind/sample-config.` se muestra un ejemplo sencillo de todo lo explicado hasta ahora.

SUGERENCIA: Adaptación automática de la información del servidor de nombres

Dependiendo del tipo de conexión a Internet o a la red, la información del servidor de nombres puede adaptarse automáticamente a las condiciones actuales. Para hacerlo, defina la variable `MODIFY_NAMED_CONF_DYNAMICALLY` del archivo `/etc/sysconfig/network/config` en `yes` (sí).

Sin embargo, no configure ningún dominio oficial hasta que la institución responsable asigne uno. Aunque cuente con su propio dominio y éste esté gestionado por el proveedor, es mejor no utilizarlo, ya que BIND no remitiría de todas formas las peticiones para este dominio. Por ejemplo, no se podría acceder al servidor Web del proveedor para este dominio.

Para iniciar el servidor de nombres, introduzca el comando `rcnamed start` como `usuario Root.` Si a la derecha aparece "done" (finalizado) en verde, querrá decir que "named", que es como se denomina al proceso del servidor de nombres, se ha iniciado correctamente. Compruebe el servidor de nombres inmediatamente en el sistema local con los programas `host` o `dig`, que deberían devolver `localhost` como servidor por defecto con la dirección `127.0.0.1`. Si este no es el caso, `/etc/resolv .conf` contiene probablemente una entrada del servidor de nombres incorrecta o el archivo no existe. Para la primera prueba, introduzca `host 127.0.0.1`, que debería funcionar siempre. Si aparece un mensaje de error, utilice `rcnamed status` para ver si el servidor se está ejecutando realmente. Si el servidor de nombres no se inicia o se comporta de manera inesperada, normalmente podrá encontrar la causa en el archivo de registro `/var/log/messages.`

Para usar el servidor de nombres del proveedor, o uno que ya se esté ejecutando en la red como remitente, introduzca la dirección o direcciones IP correspondientes en la sección `options` en la línea `forwarders`. Las direcciones incluidas en el Ejemplo 20.1, "Remisión de opciones en named.conf" (p. 407) son sólo ejemplos. Ajuste estas entradas a su propia configuración.

Ejemplo 20.1 *Remisión de opciones en named.conf*

```
options {
        directory "/var/lib/named";
        forwarders { 10.11.12.13; 10.11.12.14; };
        listen-on { 127.0.0.1; 192.168.0.99; };
        allow-query { 127/8; 192.168.0/24; };
        notify no;
        };
```

La entrada `options` está seguida de las entradas para la zona, `localhost` y `0.0.127.in-addr.arpa`. La entrada `type hint` situaba bajo el "." siempre debería estar presente. Los archivos correspondientes no tendrían que modificarse y deberían funcionar tal y como estén. Asegúrese de que cada entrada está cerrada con un punto y coma ";" y que las llaves ({ }) se encuentran en los lugares correctos. Después de cambiar el archivo de configuración `/etc/named.conf` o los archivos de zona, indique a BIND que vuelva a leerlos con `rcnamed reload`. Puede conseguir lo

mismo deteniendo y reiniciando el servidor de nombres con `rcnamed restart`. Detenga el servidor en cualquier momento introduciendo `rcnamed stop`.

20.4 Archivo de configuración /etc/named.conf

Todos los ajustes del servidor de nombres BIND se almacenan en el archivo `/etc/named.conf`. Sin embargo, los datos de zona para que se gestionan los dominios (nombres de host, direcciones IP, etc.) se almacenan en archivos independientes en el directorio `/var/lib/named`. Hay más información sobre esto más adelante.

`/etc/named.conf` se puede dividir de forma somera en dos áreas. Una es la sección `options` para los ajustes generales, y la otra consiste en entradas `zone` para los dominios individuales. La sección de `registro` y las entradas de `acl` (lista de control de acceso) son opcionales. Las líneas de comentario comienzan con el signo almohadilla # o con dos barras `//`. A continuación se muestra un archivo `/etc/named.conf` básico en el Ejemplo 20.2, “Archivo /etc/named.conf básico” (p. 408).

Ejemplo 20.2 *Archivo /etc/named.conf básico*

```
options {
        directory "/var/lib/named";
        forwarders { 10.0.0.1; };
        notify no;
};

zone "localhost" in {
       type master;
       file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
        type master;
        file "127.0.0.zone";
};

zone "." in {
        type hint;
        file "root.hint";
};
```

20.4.1 Opciones de configuración importantes

directory "*nombre de archivo*";
: Especifique el directorio en el que BIND puede encontrar los archivos que contienen los datos de la zona. Normalmente, se trata de `/var/lib/named`.

forwarders { *ip-address*; };
: Especifica los servidores de nombres (la mayoría del proveedor) a los que se deberían remitir las peticiones DNS si no pueden resolverse directamente. Sustituya *dirección ip* con una dirección IP, como `10.0.0.1`.

forward first;
: Hace que las peticiones DNS se remitan antes de que se realice un intento para resolverlas mediante los servidores de nombres raíz. En lugar de `forward first`, se puede escribir `forward only` para remitir todas las peticiones y no enviar ninguna a los servidores de nombres raíz. Esto tiene sentido para las configuraciones de cortafuegos.

listen-on port 53 { 127.0.0.1; *ip-address*; };
: Indica a BIND en qué interfaces de red y puerto se van a aceptar las consultas de clientes. No se tiene que especificar `port 53` explícitamente, porque `53` es el puerto por defecto. Introduzca `127.0.0.1` para permitir peticiones desde el host local. Si omite esta entrada completamente, se usarán por defecto todas las interfaces.

listen-on-v6 port 53 {any; };
: Indica a BIND en qué puerto debería escuchar para recibir las peticiones de cliente de IPv6. La única alternativa a `any` es `none`. Por lo que respecta a IPv6, el servidor sólo acepta direcciones comodín.

query-source address * port 53;
: Esta entrada es necesaria si un cortafuegos está bloqueando las peticiones de DNS salientes. Le indica a BIND que publique las peticiones externamente desde el puerto 53 y no desde los puertos superiores a 1024.

query-source-v6 address * port 53;
: Indica a BIND qué puerto usar para las consultas de IPv6.

allow-query { 127.0.0.1; *red*; };
: Define las redes desde las que los clientes pueden publicar las peticiones de DNS. Sustituya *red* por la dirección como, por ejemplo, `192.168.1/24`. El `/24` al final es una expresión abreviada para la máscara de red, en este caso, `255.255.255.0`.

allow-transfer ! *;;
: Controla qué hosts pueden solicitar transferencias de zona. En el ejemplo, se deniegan completamente tales peticiones mediante `! *`. Sin esta entrada, las transferencias de zona pueden solicitarse desde cualquier parte sin restricciones.

statistics-interval 0;
: Si esta entrada no está, BIND genera varias líneas de información estadística por hora en `/var/log/messages`. Defina ek valor 0 para suprimir estas estadísticas completamente, o bien establezca un intervalo en minutos.

cleaning-interval 720;
: Esta opción define con qué frecuencia borra BIND su caché. Cada vez que ocurra, se activará una entrada en `/var/log/messages`. La especificación del tiempo se realiza en minutos. El valor por defecto es 60 minutos.

interface-interval 0;
: BIND busca regularmente las interfaces de red para las interfaces nuevas o no existentes. Si el valor está definido en `0`, no se realiza y BIND sólo escucha en las interfaces detectadas al inicio. De lo contrario, el intervalo puede definirse en minutos. El valor por defecto es sesenta minutos.

notify no;
: La opción `no` impide que se informe a otros servidores de nombres de los cambios realizados en los datos de la zona o de si el servidor de nombres se reinicia.

20.4.2 Registro

En BIND puede configurarse con mucho detalle qué, cómo y dónde tiene lugar el registro. Normalmente, los ajustes por defecto deberían ser suficientes. El Ejemplo 20.3, “Entrada para inhabilitar el registro” (p. 411) muestra la forma más sencilla de dicha entrada y suprime completamente cualquier registro.

Ejemplo 20.3 *Entrada para inhabilitar el registro*

```
logging {
        category default { null; };
};
```

20.4.3 Entradas de zona

Ejemplo 20.4 *Entrada de zona para mi-dominio.de*

```
zone "mi-dominio.de" in {
      type master;
      file "mi-dominio.zone";
      notify no;
};
```

Después de `zone,` especifique el nombre del dominio que se va a administrar `(mi-dominio.de)` seguido por `in` y una serie de opciones relevantes entre llaves, tal y como se muestra en el Ejemplo 20.4, "Entrada de zona para mi-dominio.de" (p. 411). Para definir una *zona esclava,* cambie `type` a `slave` y especifique un servidor de nombres que administre esta zona como `master`, que, a su vez, puede ser un esclavo de otro principal, tal y como se muestra en el Ejemplo 20.5, "Entrada de zona para otro-dominio.de" (p. 411).

Ejemplo 20.5 *Entrada de zona para otro-dominio.de*

```
zone "otro-dominio.de" in {
      type slave;
      file "slave/otro-dominio.zone";
      masters { 10.0.0.1; };
};
```

Opciones de zona:

type master;
: Al especificar `master`, se indica a BIND que la zona está gestionada por el servidor de nombres local. De esta forma se asume que se ha creado un archivo de zona con el formato correcto.

type slave;
: Esta zona se transfiere desde otro servidor de nombres. Debe usarse junto con `masters`.

type hint;
: La zona `.` del tipo `hint` se utiliza para indicar los servidores de nombres raíz. Es una definición de zona que no es necesario modificar.

file `mi-dominio.zone` o file “slave/otro-dominio.zone”;
: Esta entrada indica el archivo que contiene los datos de zona para el dominio. En caso de un esclavo no hace falta que el archivo exista, ya que se toma de otro servidor de nombres. Para separar los archivos esclavos de los principales, utilice `slave` como directorio de los archivos esclavos.

masters { *`dirección-ip-servidor`*; };
: Esta entrada sólo es necesaria para las zonas esclavas. Indica desde qué servidor de nombres se debe transferir el archivo de zona.

allow-update {! *; };
: Esta opción regula el acceso de escritura externo, lo que permitirá a los clientes crear su propia entrada de DNS (algo que normalmente no debe hacerse por motivos de seguridad). Sin esta entrada, las actualizaciones de zona están prohibidas. La entrada mencionada anteriormente obtiene los mismos resultados porque `! *` prohíbe igualmente cualquier actividad.

20.5 Archivos de zona

Son necesarios dos tipos de archivos de zona. Uno asigna direcciones IP a nombres de host y el otro hace lo contrario: ofrece un nombre de host para una dirección IP.

SUGERENCIA: Uso del punto (.) en los archivos de zona

El punto tiene un significado importante en los archivos de zona. A todos los nombres de host que se indican sin un punto al final, se les añade la zona. Los nombres de host completos especificados con un nombre de dominio completo deben acabar en un punto para evitar que se tenga que añadir de nuevo un dominio. Si el punto falta o está en una posición equivocada puede dar lugar al error más frecuente en la configuración de un servidor de nombres.

El primer caso que vamos a explicar es el archivo de zona `world.zone`, que es el responsable del dominio `world.cosmos`. Consulte el Ejemplo 20.6, “Archivo /var/lib/named/world.zone” (p. 413).

Ejemplo 20.6 *Archivo /var/lib/named/world.zone*

```
$TTL 2D
world.cosmos. IN SOA      gateway  root.world.cosmos. (
            2003072441  ; serial
            1D          ; refresh
            2H          ; retry
            1W          ; expiry
            2D )        ; minimum

            IN NS       gateway
            IN MX       10 sun

gateway     IN A        192.168.0.1
            IN A        192.168.1.1
sun         IN A        192.168.0.2
moon        IN A        192.168.0.3
earth       IN A        192.168.1.2
mars        IN A        192.168.1.3
www         IN CNAME    moon
```

Línea 1:

`$TTL` define la duración por defecto que debería aplicarse a todas las entradas del archivo. En este ejemplo, las entradas son válidas durante un periodo de dos días `(2 D).`

Línea 2:

Aquí comienza la parte del registro de control SOA (Inicio de autoridad):

- En primer lugar figura el nombre del dominio que administrar: `world.cosmos`. Termina en punto porque, de lo contrario, se añadiría la zona otra vez. Una alternativa sería escribir el símbolo `@`, en cuyo caso la zona se extraería de la entrada correspondiente en `/etc/named.conf.`

- Detrás de `IN SOA` se encuentra el servidor de nombres que actuará como principal en esta zona. En este caso, el nombre se amplía de `gateway` a `gateway.world.cosmos` ya que no termina en punto.

- A continuación aparece la dirección de correo electrónico de la persona que se encarga de este servidor de nombres. Como el símbolo `@` ya tiene un significado especial, se reemplaza por un punto. Por tanto, para `root@world.cosmos` se debe escribir `root.world.cosmos.`. Debe incluirse un punto al final para impedir que la zona se añada.

- El paréntesis de apertura `(` incluye todas las líneas que haya en el registro SOA hasta el paréntesis de cierre `)`.

Línea 3:

El `número de serie` es un número al azar que debe aumentarse después de cada modificación del archivo. Es necesario para informar a los servidores de nombres secundarios (servidores esclavos) acerca de los cambios. El formato más común para indicarlo es mediante una cifra de 10 dígitos formada por la fecha y el número de orden en la forma AAAAMMDDNN.

Línea 4:

La `frecuencia de actualización` especifica la frecuencia con la que los servidores de nombres secundarios verifican el `número de serie` de la zona. En este caso, un día.

Línea 5:

La `frecuencia de reintento` especifica después de cuánto tiempo el servidor de nombres secundario intenta conectar nuevamente con el servidor primario en caso de error. En este caso son dos horas.

Línea 6:

La `hora de caducidad` especifica el tiempo transcurrido después del cual el servidor de nombres secundario debe desechar los datos almacenados en caché si no se ha podido restablecer el contacto con el servidor primario. En este caso es una semana.

Línea 7:

La última entrada del registro SOA especifica el `tiempo de vida (TTL) de almacenamiento en caché negativo;` es decir, el tiempo que los resultados de las consultas DNS sin resolver de otros servidores pueden almacenarse en caché.

Línea 9:

`IN NS` especifica el servidor de nombres responsable de este dominio. En este caso `gateway` se vuelve a convertir en `gateway.world.cosmos` porque no termina en punto. Puede haber varias líneas de este tipo, una para el servidor de nombres primario y otra para cada servidor de nombres secundario. Si la variable `notify` no está definida en `no` en `/etc/named.conf`, se informará a todos los servidores de nombres aquí mencionados de los cambios en los datos de zona.

Línea 10:

El registro MX indica el servidor de correo que acepta, procesa y remite los mensajes de correo electrónico al dominio `world.cosmos`. En este ejemplo, se trata del host `sun.world.cosmos`. El número situado delante del nombre del host se corresponde con el valor de preferencia. Si existen varias entradas MX, primero se utiliza el servidor de correo con el valor de preferencia más bajo y, si la entrega del correo a este servidor no se produce, se hará un intento con el valor inmediatamente superior.

Líneas 12 a 17:

Se corresponden con los registros de direcciones reales en los que una o varias direcciones IP se asignan a nombres de host. Todos los nombres aparecen sin un punto porque no incluyen el dominio, de tal forma que `world.cosmos` se añadirá a todos ellos. Las dos direcciones IP se asignan al host `gateway` porque cuenta con dos tarjetas de red. Allí donde la dirección del host es de tipo tradicional (IPv4), el registro aparece marcado con una A. Si la dirección es una dirección IPv6, la entrada aparece marcada con A6. El testigo anterior para las direcciones IPv6 era AAAA, que ahora está obsoleto.

NOTA: Sintaxis A6

Los registros A6 tienen una sintaxis ligeramente distinta a AAAA. Debido a que existe la posibilidad de fragmentación, es necesario ofrecer información acerca de los bits que faltan antes de la dirección. Debe ofrecer esta información incluso si desea usar una dirección completamente desfragmentada. En el caso del registro AAAA antiguo, con la sintaxis siguiente:

```
pluto IN            AAAA 2345:00C1:CA11:0001:1234:5678:9ABC:DEF0
 pluto IN            AAAA 2345:00D2:DA11:0001:1234:5678:9ABC:DEF0
```

Tiene que añadir información acerca de los bits que faltan cuando lo haga en formato A6. Debido a que el ejemplo de arriba está completo (no falta ningún bit), el formato A6 de este registro será:

```
pluto  IN            AAAA 0 2345:00C1:CA11:0001:1234:5678:9ABC:DEF0
 pluto  IN            AAAA 0 2345:00D2:DA11:0001:1234:5678:9ABC:DEF0
```

No use direcciones IPv4 con la asignación de IPv6. Si un host cuenta con una dirección IPv4, utilizará un registro A no uno A6.

Línea 18:
: Se puede utilizar el alias `www` para acceder a `mond` (`CNAME` significa *nombre canónico*).

Para la resolución inversa de direcciones IP en nombres de host, se utiliza el seudodominio `in-addr.arpa.` Se añadirá al final de la parte correspondiente a la red de la dirección escrita en orden inverso. De tal forma que `192.168.1` se convierte en `1.168.192.in-addr.arpa`. Consulte el Ejemplo 20.7, "Resolución inversa" (p. 416).

Ejemplo 20.7 *Resolución inversa*

```
$TTL 2D
1.168.192.in-addr.arpa. IN SOA gateway.world.cosmos. root.world.cosmos. (
                        2003072441      ; serial
                        1D              ; refresh
                        2H              ; retry
                        1W              ; expiry
                        2D )            ; minimum

                        IN NS           gateway.world.cosmos.

1                       IN PTR          gateway.world.cosmos.
2                       IN PTR          earth.world.cosmos.
3                       IN PTR          mars.world.cosmos.
```

Línea 1:
: $TTL define el tiempo de vida (TTL) estándar que se aplica a todas las entradas.

Línea 2:
: El archivo de configuración debería activar la resolución inversa para la red `192.168.1.0`. Puesto que la zona se denomina `1.168.192.in-addr.arpa`, no deberían añadirse a los nombres de host. Por lo tanto, todos estos se introducirán con la forma completa; es decir, con el dominio y el punto al final. Las entradas que queden se corresponderán con las descritas en el ejemplo anterior de `world.cosmos`.

Líneas 3 a 7:
: Consulte el ejemplo anterior de `world.cosmos`.

Línea 9:
: Esta línea indica el servidor de nombres responsable de esta zona. No obstante, en este caso el nombre se introduce con su nombre completo, o sea, con el dominio y el punto al final.

Líneas 11 a 13:
: Hay registros de puntero que llevan a las direcciones IP de los hosts correspondientes. Al principio de la línea sólo se introduce la última parte de la dirección IP, sin el punto al final. Al añadir la zona al final (sin `.in-addr.arpa`) dará como resultado la dirección IP completa en orden inverso.

Por lo general, las transferencias de zonas entre versiones distintas de BIND no deberían representar ningún problema.

20.6 Actualización dinámica de los datos de zona

El término *actualización dinámica* se emplea para describir operaciones relacionadas con las entradas añadidas, modificadas o suprimidas en los archivos de zonas de un servidor principal. Este mecanismo está descrito en la norma RFC 2136. La actualización dinámica se configura individualmente para cada entrada de zona al añadir reglas opcionales del tipo `allow-update` o `update-policy`. Las zonas que se actualicen dinámicamente no deberían editarse de forma manual.

Transmita al servidor las entradas que han de actualizarse con el comando `nsupdate`. Consulte la sintaxis exacta de este comando en la página Man de nsupdate (`man 8 nsupdate`). Por motivos de seguridad, la actualización debería realizarse a través de las claves TSIG tal y como se describe en la Sección 20.7, “Transacciones seguras” (p. 417).

20.7 Transacciones seguras

Las transacciones seguras pueden realizarse mediante firmas de transacción (TSIG), que se basan en claves secretas compartidas (también denominadas "claves TSIG"). En esta sección se describe cómo generar y utilizar tales claves.

Las transacciones seguras son necesarias para la comunicación entre servidores y para actualizar los datos de zona dinámicamente. En este contexto, un control de acceso basado en claves es mucho más seguro que un control basado en direcciones IP.

Genere una clave TSIG con el comando siguiente (para obtener información detallada, consulte `man dnssec-keygen`):

```
dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2
```

Al ejecutar este comando se crearán dos archivos con nombres parecidos a estos:

```
Khost1-host2.+157+34265.private Khost1-host2.+157+34265.key
```

La clave propiamente dicha (por ejemplo, `ejIkuCyyGJwwuN3xAteKgg==`) se encuentra en ambos archivos. Para usarla en transacciones, el segundo archivo (`Khost1-host2.+157+34265.key`) debe transferirse al host remoto, preferiblemente de manera segura (por ejemplo, usando scp). En el servidor remoto, la clave debe incluirse en el archivo `/etc/named.conf` para permitir la comunicación segura entre el `host1` y el `host2`:

```
key host1-host2. {
 algorithm hmac-md5;
 secret ";ejIkuCyyGJwwuN3xAteKgg==;
};
```

AVISO: Permisos de archivo de `/etc/named.conf`

Asegúrese de que los permisos de `/etc/named.conf` estén restringidos convenientemente. El valor por defecto de este archivo es `0640`, el propietario es el usuario `Root` y el grupo `named`. También es posible mover las claves a un archivo independiente con permisos limitados de manera específica que se incluirían en `/etc/named.conf`.

Para permitir que el servidor `host1` use la clave para `host2` (con la dirección `192.168.2.3` en este ejemplo), el archivo `/etc/named.conf` del servidor debe incluir la regla siguiente:

```
server 192.168.2.3 {
  keys { host1-host2. ;};
};
```

Se deben incluir entradas parecidas en los archivos de configuración de `host2`.

Añada claves TSIG para cualquier ACL (lista de control de acceso, no confundirlas con las ACL del sistema de archivos) que se defina para las direcciones IP y los inter-

valos de direcciones, con objeto de habilitar la seguridad de la transacción. La entrada correspondiente podría ser más o menos así:

```
allow-update { key host1-host2. ;};
```

Obtenga información más detallada sobre este tema en el *BIND Administrator Reference Manual* (Manual de referencia del administrador de BIND), en la sección `update-policy`.

20.8 Seguridad DNS

La DNSSEC, o lo que es lo mismo "seguridad DNS", se describe en la norma RFC 2535. Las herramientas disponibles para utilizar DNSSEC se describen en el manual de BIND.

Una zona segura debe contar con una o varias claves de zona asociadas a ella. Se generan mediante `dnssec-keygen`, al igual que las claves de host. El algoritmo de cifrado de DSA se utiliza actualmente para generar estas claves. Las claves públicas generadas deberían incluirse en el archivo de zona correspondiente mediante una regla `$INCLUDE`.

Gracias al comando `dnssec-makekeyset`, todas las claves generadas se agrupan en un conjunto, que debe transferirse a continuación a la zona principal de una manera segura. En la zona principal, el conjunto se firma con `dnssec-signkey`. Los archivos generados por este comando se utilizarán para firmar zonas con el comando `dnssec-signzone`, que, a su vez, genera los archivos que se incluirán en cada zona en `/etc/named.conf`.

20.9 Información adicional

Para obtener información adicional, consulte el *BIND Administrator Reference Manual* (Manual de referencia del administrador de BIND) incluido en el paquete `bind-doc`, que se instala en `/usr/share/doc/packages/bind/`. Considere la posibilidad de consultar las normas RFC a las que se hace referencia en el manual, así como las páginas Man incluidas con BIND. `/usr/share/doc/packages/bind/README.SuSE` contiene información actualizada acerca de BIND en SUSE Linux.

21 Uso de NIS

Cuando varios sistemas UNIX de una red desean acceder a recursos comunes, es fundamental que todas las identidades de usuario y de grupo sean las mismas para todas las máquinas de dicha red. La red debe ser transparente para los usuarios: independientemente de la máquina que utilicen, siempre deben encontrarse en el mismo entorno. Esto es posible gracias a los servicios NIS y NFS. NFS distribuye sistemas de archivos a lo largo de una red y se describe en el Capítulo 22, *Uso compartido de sistemas de archivos con NFS* (p. 431).

El servicio NIS (Servicio de información de red) se puede describir como un servicio de base de datos que proporciona acceso a los contenidos de `/etc/passwd`, `/etc/shadow` y `/etc/group` a lo largo de redes. El servicio NIS también se puede utilizar para otros propósitos (por ejemplo, para la disponibilidad de los contenidos de archivos `/etc/hosts` o `/etc/services`), pero esto no se incluye en la presente introducción. También se hace referencia al servicio NIS como *YP*, puesto que funciona como la red de las “páginas amarillas”.

21.1 Configuración de los servidores NIS

Para distribuir la información de NIS por las redes, puede tener un único servidor (uno *principal*) que sirva a todos los clientes, o bien puede tener servidores NIS esclavos que pidan esta información al servidor principal, que a su vez lo reenvía a sus respectivos clientes.

- Para configurar sólo un servidor NIS para la red, realice las acciones especificadas en la Sección 21.1.1, “Configuración de un servidor NIS principal” (p. 422).
- Si el servidor NIS principal debe exportar los datos a los servidores esclavos en otras subredes, configure el servidor principal tal y como se describe en la Sección 21.1.1, “Configuración de un servidor NIS principal” (p. 422) y configure los servidores esclavos en las subredes tal y como se explica en la Sección 21.1.2, “Configuración de un servidor NIS esclavo” (p. 427).

21.1.1 Configuración de un servidor NIS principal

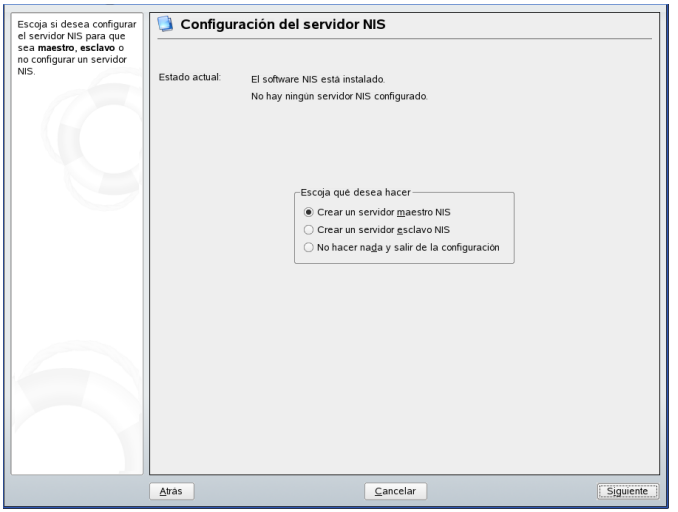
Para configurar un servidor NIS principal para la red, proceda de la siguiente manera:

1. Inicie *YaST → Servicios de red → Servidor NIS*.
2. Si sólo necesita un servidor NIS en la red o si este servidor va a actuar como servidor principal de los servidores NIS esclavos, seleccione *Instalar y configurar un servidor maestro NIS*. YaST instalará los paquetes necesarios.

SUGERENCIA

Si el software del servidor NIS ya está instalado en el equipo, inicie la creación de un servidor NIS principal haciendo clic en *Crear un servidor maestro NIS*.

Figura 21.1 *Configuración del servidor NIS*



3 Determine las opciones de configuración básicas de NIS:

a Introduzca el nombre de dominio de NIS.

b Defina si el host debería ser un cliente NIS, lo que permitiría que los usuarios iniciaran sesión y accedieran a los datos desde el servidor NIS seleccionando *Este equipo es también un cliente NIS*.

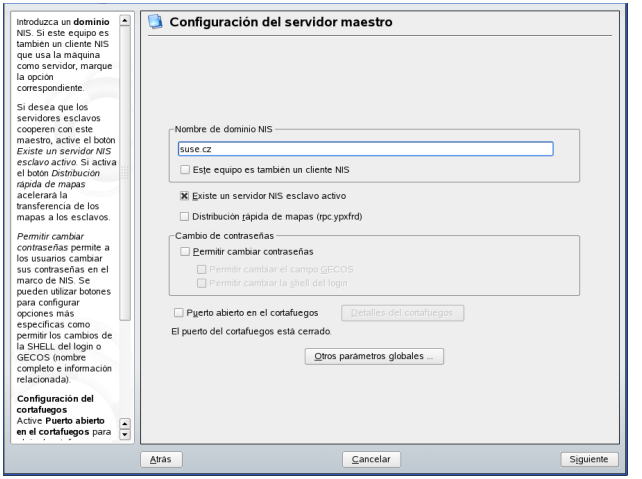
Seleccione *Cambio de contraseñas* para permitir que los usuarios de la red (tanto usuarios locales como aquellos que se gestionan mediante el servidor NIS) cambien sus contraseñas en el servidor NIS (con el comando `yppasswd`).

Esto pondrá a su disposición las opciones *Allow Changes to GECOS Field* (Permitir cambios en el campo GECOS) y *Allow Changes to Login Shell* (Permitir cambios en la shell de login). “GECOS” significa que los usuarios también pueden cambiar sus nombres y direcciones con el comando `ypchfn`. “SHELL” permite a los usuarios cambiar la shell por defecto con el comando `ypchsh`, por ejemplo para cambiar de bash a sh. La nuevo shell debe ser una de las entradas predefinidas en `/etc/shells`.

c Si el servidor NIS debe actuar como un servidor principal para los servidores NIS esclavos en otras subredes, seleccione *Existe un servidor NIS esclavo activo*.

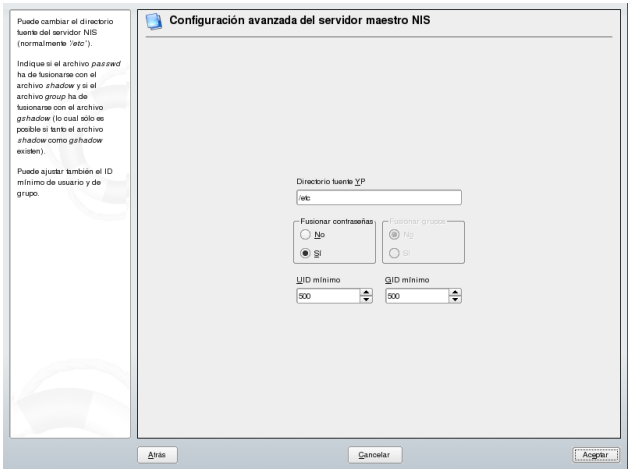
d Seleccione *Puerto abierto en el cortafuegos* para que YaST adapte los ajustes del cortafuegos para el servidor NIS.

Figura 21.2 *Configuración del servidor principal*



e Salga de este cuadro de diálogo haciendo clic en *Siguiente* o haga clic en *Otros parámetros globales* para realizar los ajustes adicionales. La opción *Otros parámetros globales* incluye el cambio del directorio de origen del servidor NIS (`/etc` por defecto). Además, las contraseñas pueden fusionarse aquí. El ajuste debe ser *Sí* para que se utilicen los archivos (`/etc/passwd`, `/etc/shadow` y `/etc/group`) para generar la base de datos del usuario. Además, determine los ID de usuario y de grupo más pequeños que debe ofrecer NIS. Haga clic en *Aceptar* para confirmar los ajustes y volver a la pantalla anterior.

Figura 21.3 *Cambio de directorio y sincronización de archivos para un servidor NIS*

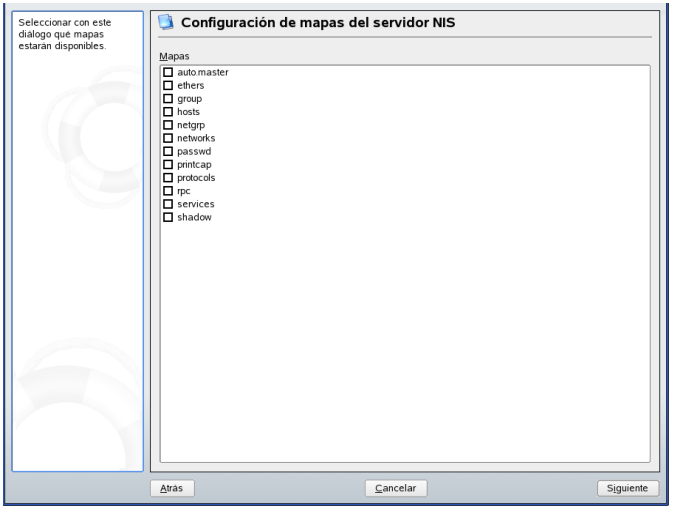


4 Si ya ha habilitado *Existe un servidor NIS esclavo activo*, introduzca los nombres de host utilizados y haga clic en *Siguiente*.

5 Si no utiliza servidores esclavos, la configuración del esclavo se omitirá y aparecerá directamente el cuadro de diálogo de configuración de la base de datos. Especifique las *asignaciones*, es decir, las bases de datos que desee transferir desde el servidor NIS al cliente. Generalmente, basta con la configuración por defecto. Salga del cuadro de diálogo con *Siguiente.*

6 Compruebe las asignaciones que deberían estar disponibles y haga clic en *Siguiente* para continuar.

Figura 21.4 *Configuración de las asignaciones del servidor NIS*

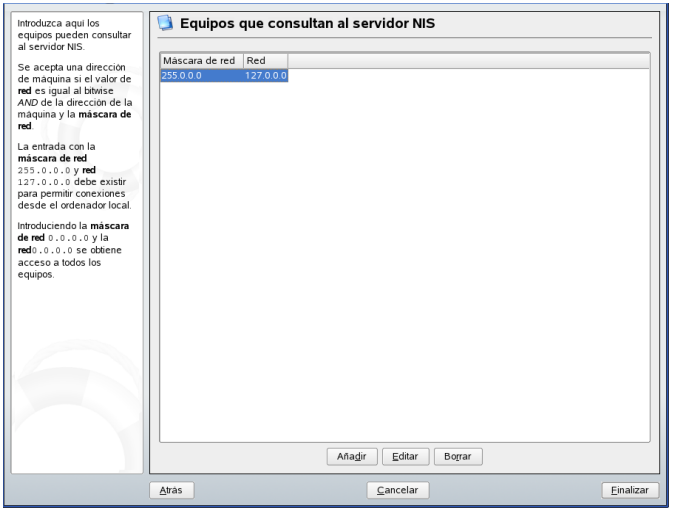


7 Introduzca los hosts que tienen permiso para realizar consultas al servidor NIS. Puede agregar, editar o suprimir hosts haciendo clic en los botones correspondientes. Especifique las redes que pueden emitir peticiones al servidor NIS. Normalmente, se trata de la red interna. En este caso, deben aparecer las dos entradas siguientes:

```
255.0.0.0       127.0.0.0
0.0.0.0         0.0.0.0
```

La primera entrada habilita las conexiones desde su propio host que es el servidor NIS. La segunda permite a todos los hosts enviar peticiones al servidor.

Figura 21.5 *Configuración de permisos de petición para un servidor NIS*



8 Haga clic en *Finalizar* para guardar los cambios y salir de la configuración.

21.1.2 Configuración de un servidor NIS esclavo

Para configurar *servidores NIS esclavos* adicionales en la red, realice lo siguiente:

1 Inicie *YaST → Servicios de red → Servidor NIS*.

2 Seleccione *Instalar y configurar un servidor esclavo NIS* y haga clic en *Siguiente*.

SUGERENCIA

Si el software del servidor NIS ya está instalado en el equipo, inicie la creación de un servidor NIS esclavo haciendo clic en *Crear un servidor esclavo NIS*.

3 Complete la configuración básica del servidor NIS esclavo:

a Introduzca el dominio de NIS.

b Introduzca el nombre de host y la dirección IP del servidor principal.

c Marque la opción *Este equipo es también un cliente NIS* si desea habilitar los inicios de sesión de los usuarios en este servidor.

d Adapte los ajustes del cortafuegos con *Puerto abierto en el cortafuegos.*

e Haga clic en *Siguiente.*

4 Introduzca los hosts que tienen permiso para realizar consultas al servidor NIS. Puede agregar, editar o suprimir hosts haciendo clic en los botones correspondientes. Especifique las redes que pueden emitir peticiones al servidor NIS. Normalmente, son todos hosts. En este caso, deben aparecer las dos entradas siguientes:

```
255.0.0.0     127.0.0.0
0.0.0.0       0.0.0.0
```

La primera entrada habilita las conexiones desde su propio host que es el servidor NIS. La segunda permite a todos los hosts con acceso a la misma red enviar peticiones al servidor.

5 Haga clic en *Finalizar* para guardar los cambios y salir de la configuración.

21.2 Configuración de clientes NIS

Utilice el módulo *Cliente NIS* para configurar una estación de trabajo con la que usar NIS. Seleccione si el host posee una dirección IP estática o si recibe una procedente de DHCP. DHCP también puede proporcionar el dominio y el servidor NIS. Para obtener más información acerca de DHCP, consulte el Capítulo 23, *DHCP* (p. 439). Si se utiliza una dirección IP estática, indique el dominio NIS y el servidor NIS manualmente. Consulte la Figura 21.6, “Configuración de dominio y dirección de un servidor NIS” (p. 429). La opción *Buscar* realiza una búsqueda YaST de un servidor NIS activo en la red. Según el tamaño de la red local, puede ser un proceso que lleve mucho tiempo. La opción *Difusión* busca un servidor NIS en la red local después de no haber obtenido una respuesta de los servidores especificados.

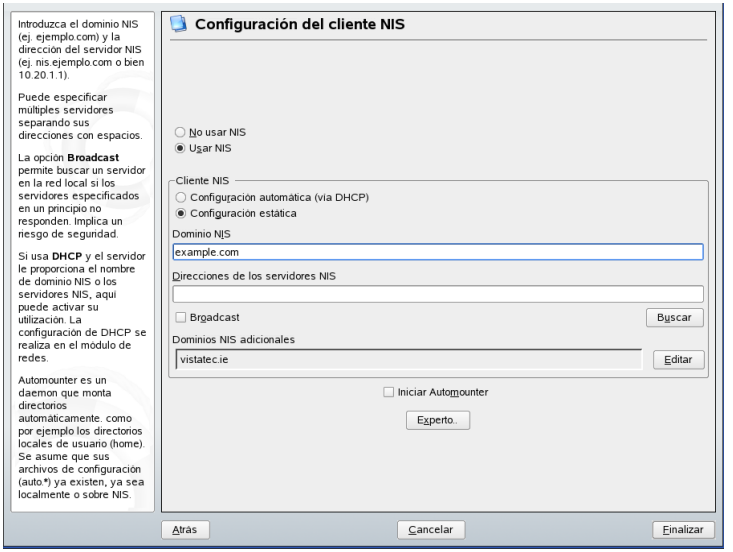
También puede especificar varios servidores introduciendo las direcciones en *Direcciones de los servidores NIS* y separándolos con espacios.

Dependiendo de la instalación local, podrá activar también el montador automático. Esta opción también instalará el software adicional si fuera preciso.

En la configuración avanzada, inhabilite *Responder a máquinas remotas* si no desea que otros hosts puedan consultar el servidor utilizado por el cliente. Al marcar *Servidor roto*, el cliente está habilitado para recibir respuestas desde un servidor que se comunica a través de un puerto no privilegiado. Para obtener más información, consulte `man ypbind`.

Después de realizar la configuración, haga clic en *Finalizar* para guardarla y volver al Centro de control de YaST.

Figura 21.6 *Configuración de dominio y dirección de un servidor NIS*



Uso compartido de sistemas de archivos con NFS

22

Tal y como se comenta en el Capítulo 21, *Uso de NIS* (p. 421), NFS trabaja con NIS para que la red resulte transparente al usuario. Mediante NFS es posible distribuir sistemas de archivos a través de la red. No importa en qué terminal hayan iniciado sesión los usuarios. Siempre se encuentran con un mismo entorno.

Al igual que NIS, NFS es un sistema cliente/servidor. Una misma máquina puede ser ambos (puede proporcionar sistemas de archivos a la red [exportar] y montar sistemas de archivos de otros hosts [importar]).

IMPORTANTE: Necesidad de DNS

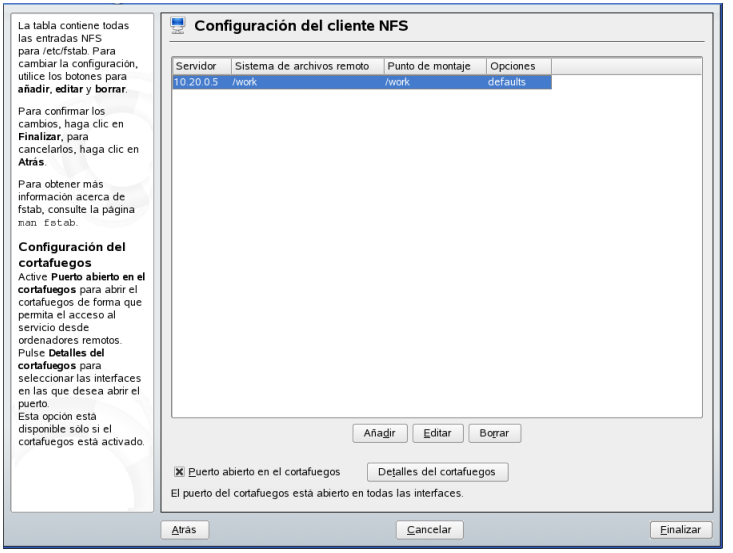
En principio, las exportaciones se pueden realizar usando sólo direcciones IP. Sin embargo, para evitar superar los tiempos límites, debe haber un sistema DNS funcionando. Esto es necesario al menos a efectos de registro, ya que el daemon mountd realiza búsquedas inversas.

22.1 Importación de sistemas de archivos con YaST

Para ello, los usuarios autorizados pueden montar directorios NFS a partir de un servidor NFS en sus propios árboles de archivos. La manera más sencilla de hacerlo es mediante el módulo *Cliente NFS* de YaST. Sólo hay que introducir el nombre de host del servidor NFS, el directorio en el que se importará y el punto de montaje en el que se montará este directorio localmente. Para ello, haga clic en *Añadir* en el primer cuadro de diálogo.

Haga clic en *Puerto abierto en el cortafuegos* para abrir el cortafuegos y permitir el acceso al servicio desde equipos remotos. El estado del cortafuegos se muestra junto a la casilla de verificación. Haga clic en *Aceptar* para guardar los cambios. Consulte la Figura 22.1, “Configuración de clientes NFS con YaST” (p. 432).

Figura 22.1 *Configuración de clientes NFS con YaST*



22.2 Importación manual de sistemas de archivos

Los sistemas de archivos se pueden importar manualmente de forma sencilla desde un servidor NFS. El único requisito previo es la ejecución de un asignador de puertos RPC, que puede iniciarse introduciendo el comando `rcportmap start` como usuario `root`. Una vez cumplido este requisito previo, los sistemas de archivos remotos exportados a las máquinas respectivas se pueden montar en el sistema de archivos exactamente igual que los discos duros locales mediante el comando `mount` con la siguiente sintaxis:

```
mount host:remote-path local-path
```

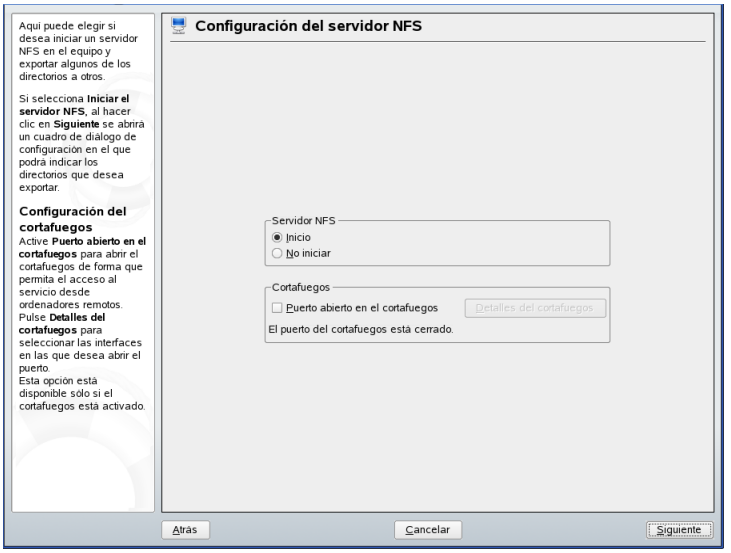
Por ejemplo, para importar los directorios de usuario de la máquina sun, se utilizaría el siguiente comando:

```
mount sun:/home /home
```

22.3 Exportación de sistemas de archivos con YaST

Con YaST es posible convertir un host de la red en un servidor NFS (un servidor que exporta directorios y archivos a todos los hosts a los que se conceda acceso). Esto puede hacerse, por ejemplo, para ofrecer aplicaciones a todos los miembros de un grupo sin tener que instalarlas de manera local en todos y cada uno de los hosts. Para instalar este servidor, inicie YaST y seleccione *Servicios de red* → *Servidor NFS*. Se abrirá un cuadro de diálogo como el que se muestra en la Figura 22.2, “Herramienta de configuración del servidor NFS” (p. 433).

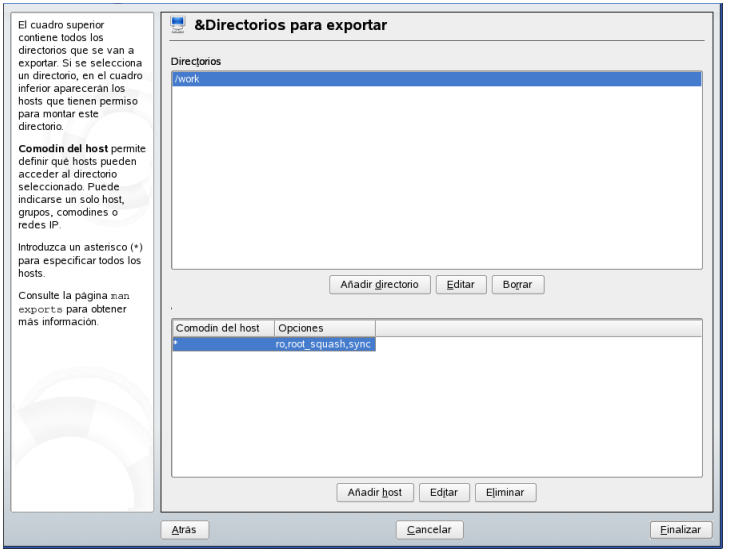
Figura 22.2 *Herramienta de configuración del servidor NFS*



A continuación, active *Iniciar el servidor NFS* y haga clic en *Siguiente*. En el campo de texto superior, introduzca los directorios que se exportarán. A continuación, introduzca los hosts que tendrán acceso a ellos. Este cuadro de diálogo se muestra en la

Figura 22.3, “Configuración de un servidor NFS con YaST” (p. 434). Para cada host se pueden establecer cuatro opciones: `equipo único`, `grupos de trabajo en red`, `comodines` y `redes IP`. Puede acceder a una explicación más detallada de estas opciones con `man exports`. La configuración se finaliza mediante *Salir*.

Figura 22.3 *Configuración de un servidor NFS con YaST*



IMPORTANTE: Configuración automática del cortafuegos

Si hay un cortafuegos activo en el sistema (SuSEfirewall2), YaST adaptará su configuración para el servidor NFS habilitando el servicio `nfs` al seleccionar *Open Ports in Firewall* (Abrir puertos en el cortafuegos).

22.4 Exportación manual de sistemas de archivos

Si no desea utilizar YaST, asegúrese de que los siguientes sistemas se ejecutan en el servidor NFS:

- Asignador de puertos RPC (portmap)

- Daemon de montaje RPC (rpc.mountd)
- Daemon NFS RPC (rpc.nfsd)

Para que los guiones `/etc/init.d/portmap` y `/etc/init.d/nfsserver` inicien estos servicios al arrancar el sistema, introduzca los comandos `insserv /etc/init.d/nfsserver` e `insserv /etc/init.d/portmap`. Defina también qué sistemas de archivos deben exportarse a cada host del archivo de configuración `/etc/exports`.

Es necesaria una línea para cada directorio que se exporte en la que se establezca qué máquinas pueden acceder a él y con qué permisos. Automáticamente se exportan también todos los subdirectorios del directorio. Normalmente se especifican las máquinas autorizadas con sus nombres completos (incluido el nombre de dominio), aunque es posible utilizar comodines como `*` o `?` (que se expanden de la misma manera que en la shell Bash). Si no se especifica ninguna máquina, no se permitirá que ningún equipo importe el sistema de archivos con los permisos indicados.

Especifique entre paréntesis después del nombre de la máquina los permisos del sistema de archivos que se exportará. Las opciones más importantes se muestran en la Tabla 22.1, "Permisos para sistemas de archivos exportados" (p. 435).

Tabla 22.1 *Permisos para sistemas de archivos exportados*

Opción	Significado
`ro`	El sistema de archivos se exporta con permiso de sólo lectura (opción por defecto).
`rw`	El sistema de archivos se exporta con permiso de lectura y escritura.
`root_squash`	Esta opción garantiza que el usuario `root` de la máquina de importación no tenga privilegios de usuario `root` sobre este sistema de archivos. Ello se consigue asignando el ID de usuario`65534` a los usuarios con ID de usuario `0` (`root`). Este ID de usuario debe establecerse como `nobody` (que es la opción por defecto).

Opción	Significado
`no_root_squash`	No asigna el ID de usuario `0` al ID de usuario `65534`, con lo que los permisos de usuario `root` mantienen su validez.
`link_relative`	Convierte los enlaces absolutos (los que empiezan por `/`) en una secuencia `../`. Esto sólo resulta útil si se monta el sistema de archivos completo de una máquina (opción por defecto).
`link_absolute`	Los enlaces simbólicos no se modifican.
`map_identity`	Los IDs de usuario son exactamente los mismos en cliente y servidor (opción por defecto).
`map_daemon`	Los IDs de usuario de cliente y servidor no se corresponden. Esto indica a nfsd que cree una tabla de conversión para los IDs de usuario. Para que funcione es necesario el daemon ugidd.

El archivo `exports` puede tener un aspecto similar al del Ejemplo 22.1, "/etc/exports" (p. 436). mountd y nfsd leen `/etc/exports`. Si cambia algo en dicho archivo, reinicie mountd y nfsd para que los cambios surtan efectos. Puede hacerlo fácilmente mediante `rcnfsserver restart`.

Ejemplo 22.1 */etc/exports*

```
#
# /etc/exports
#
/home            sun(rw)   venus(rw)
/usr/X11         sun(ro)   venus(ro)
/usr/lib/texmf   sun(ro)   venus(rw)
/                earth(ro,root_squash)
/home/ftp        (ro)
# End of exports
```

22.5 Información adicional

Hay más información disponible acerca de la configuración de los servidores NFS en `/usr/share/doc/packages/nfs-utils/README` y en los documentos que allí aparecen. La documentación técnica detallada está disponible en línea en `http://nfs.sourceforge.net/`.

23 DHCP

El objetivo del *dynamic host configuration protocol* (DHCP) (protocolo de configuración dinámica de hosts) es asignar ajustes de red de manera centralizada a partir de un servidor en lugar de configurarlos localmente en cada estación de trabajo. Los hosts configurados para utilizar DHCP no tienen control sobre su propia dirección estática. Ésta se configura completa y automáticamente de acuerdo con las instrucciones del servidor. Si utiliza NetworkManager en el cliente, no tendrá que configurar el cliente en absoluto, lo que resulta útil si dispone de entornos cambiantes con sólo una interfaz activa al mismo tiempo. No utilice nunca NetworkManager en un equipo en el que se ejecute un servidor DHCP.

Una manera de configurar un servidor DHCP consiste en identificar cada cliente mediante la dirección de hardware de su tarjeta de red (la cual es fija en la mayoría de los casos) y proporcionar a cada cliente los mismos ajustes cada vez que se conecte al servidor. También se puede configurar DHCP para que se asignen direcciones a los clientes interesados de manera dinámica a partir de un conjunto de direcciones definido para este propósito. En este último caso, el servidor DHCP intenta asignar la misma dirección a cada cliente cada vez que recibe una petición por su parte, incluso a lo largo de grandes periodos de tiempo. Esto sólo funciona si la red no tiene más clientes que direcciones.

DHCP facilita el trabajo a los administradores del sistema. Cualquier cambio relacionado con las direcciones y con la configuración de la red en general, incluso los cambios más complicados, pueden implementarse de manera central mediante la edición del archivo de configuración del servidor. Esto resulta mucho más práctico que volver a configurar cada estación de trabajo cuando son muchas También resulta más fácil integrar las máquinas, y en especial las nuevas máquinas, en la red, ya que se les puede proporcionar una dirección IP del conjunto de direcciones. La obtención de los ajustes

de red apropiados a partir de un servidor DHCP es especialmente útil para equipos portátiles que se utilicen con frecuencia en redes distintas.

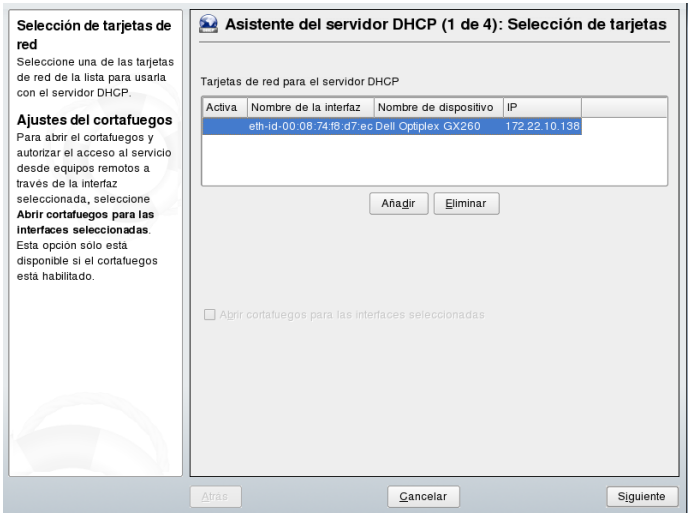
Los servidores DHCP no sólo proporcionan la dirección IP y la máscara de red, sino también el nombre de host, el nombre del dominio, el gateway y el nombre del servidor de direcciones que debe utilizar el cliente. Además, DHCP permite configurar numerosos parámetros adicionales de manera centralizada, por ejemplo, un servidor horario a partir del cual los clientes pueden obtener la hora, e incluso un servidor de impresión.

23.1 Configuración de un servidor DHCP con YaST

Al iniciar el módulo por primera vez, se muestra un asistente que solicita que tome algunas decisiones básicas relativas a la administración del servidor. Cuando se completa esta configuración inicial, se obtiene una configuración del servidor muy básica que debe funcionar en los aspectos más esenciales. Se puede utilizar el modo avanzado para realizar tareas de configuración más precisas.

Selección de tarjetas
: En el primer paso, YaST busca las interfaces de red disponibles en el sistema y las muestra en una lista. En la lista, seleccione la interfaz en la que debe escuchar el servidor DHCP y haga clic en *Añadir*. Después, seleccione *Abrir cortafuegos para las interfaces seleccionadas* para abrir el cortafuegos para esa interfaz. Consulte la Figura 23.1, “Servidor DHCP: Selección de tarjetas” (p. 441).

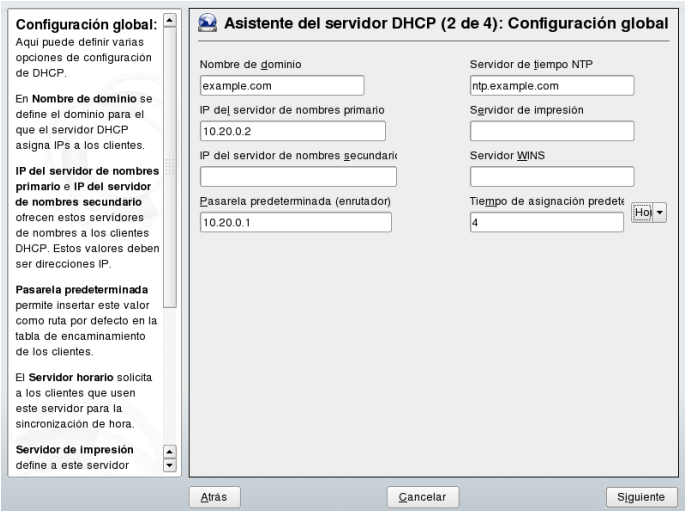
Figura 23.1 *Servidor DHCP: Selección de tarjetas*



Ajustes globales

En los campos de entrada, introduzca las especificaciones que el servidor DHCP debería gestionar para todos los clientes. Dichas especificaciones son el nombre del dominio, la dirección del servidor horario, las direcciones de los servidores de nombres primario y secundario, las direcciones de los servidores de impresión y WINS (para redes mixtas, con clientes tanto Windows como Linux), la dirección del gateway y el tiempo de asignación. Consulte la Figura 23.2, “Servidor DHCP: Ajustes globales” (p. 442).

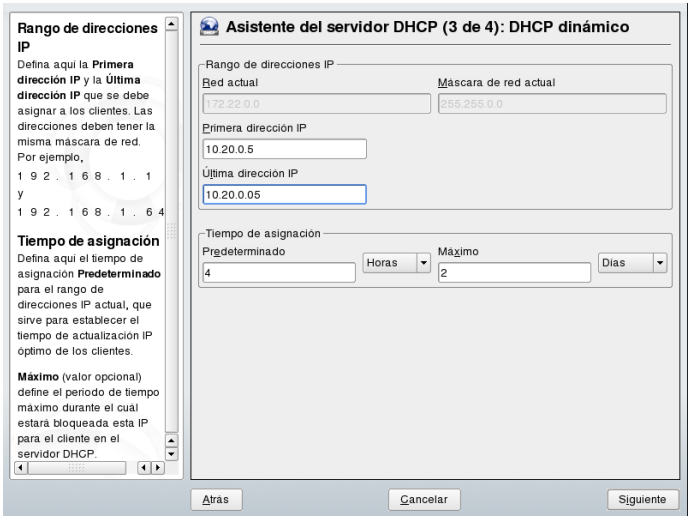
Figura 23.2 *Servidor DHCP: Ajustes globales*



DHCP dinámico

En este paso, configure cómo deben asignarse a los clientes las direcciones IP dinámicas. Para ello, especifique un rango de IP a partir del cual el servidor puede asignar direcciones a los clientes DHCP. Todas las direcciones deben quedar cubiertas por la misma máscara de red. Especifique también el tiempo de asignación durante el cual el cliente puede mantener su dirección IP sin necesidad de pedir una extensión de la asignación. De manera opcional, especifique el tiempo máximo de asignación (el periodo durante el cual el servidor reserva una dirección IP para un cliente concreto). Consulte la Figura 23.3, “Servidor DHCP: DHCP dinámico” (p. 443).

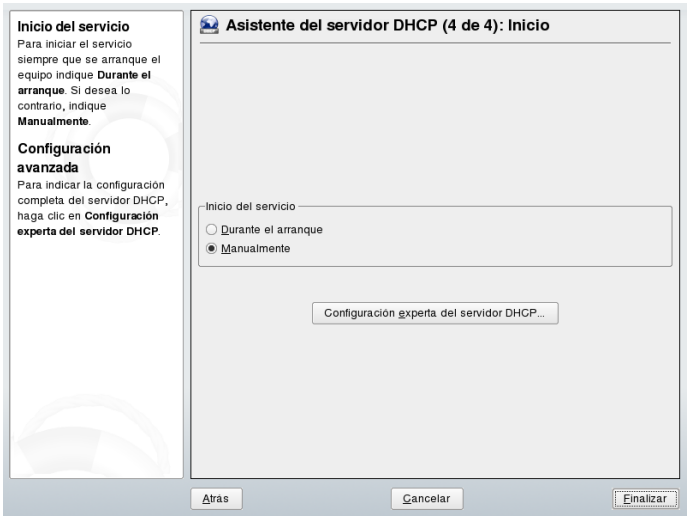
Figura 23.3 *Servidor DHCP: DHCP dinámico*



Finalización de la configuración y establecimiento del modo de inicio

Una vez completada la tercera parte del asistente de configuración, aparecerá un último cuadro de diálogo en el que es posible definir cómo debe iniciarse el servidor DHCP. Especifique en él si el servidor DHCP se iniciará automáticamente al arrancar el sistema o si se iniciará de forma manual cuando sea necesario (por ejemplo, para realizar pruebas). Haga clic en *Finalizar* para completar la configuración del servidor. Consulte la Figura 23.4, “Servidor DHCP: Inicio” (p. 444).

Figura 23.4 *Servidor DHCP: Inicio*



23.2 Paquetes de software DHCP

Para SUSE Linux se encuentran disponibles un servidor DHCP y varios clientes DHCP. El servidor DHCP disponible es dhcpd (publicado por el Internet Software Consortium). Por otro lado, se puede escoger entre dos programas cliente DHCP distintos: dhclient (también del ISC) y el daemon cliente DHCP del paquete `dhcpcd`.

SUSE Linux instala dhcpcd por defecto. El programa es muy sencillo de manejar y se ejecuta automáticamente en cada arranque del sistema para buscar un servidor DHCP. No necesita archivos de configuración para realizar sus tareas y funciona tal cual en la mayoría de las configuraciones estándar. Para entornos más complejos, utilice dhclient del ISC, que se controla por medio del archivo de configuración `/etc/dhclient.conf`.

23.3 El servidor DHCP dhcpd

El núcleo de todo sistema DHCP es el daemon del protocolo de configuración dinámica de hosts. Este servidor *asigna* direcciones y controla su utilización según los ajustes definidos en el archivo de configuración `/etc/dhcpd.conf`. El administrador del

sistema puede cambiar el comportamiento del programa de diversas maneras modificando los parámetros y los valores de dicho archivo. Observe un ejemplo básico del archivo `/etc/dhcpd.conf` en el Ejemplo 23.1, "El archivo de configuración /etc/dhcpd.conf" (p. 445).

Ejemplo 23.1 *El archivo de configuración /etc/dhcpd.conf*

```
default-lease-time 600;         # 10 minutes
max-lease-time 7200;            # 2  hours

option domain-name "cosmos.all";
option domain-name-servers 192.168.1.1, 192.168.1.2;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option subnet-mask 255.255.255.0;

subnet 192.168.1.0 netmask 255.255.255.0
 {
  range 192.168.1.10 192.168.1.20;
  range 192.168.1.100 192.168.1.200;
 }
```

Este sencillo archivo de configuración debería ser suficiente para conseguir que el servidor DHCP asignara direcciones IP en la red. Asegúrese de que haya un punto y coma al final de cada línea, ya que de lo contrario el servidor dhcpd no se iniciará.

El archivo de ejemplo anterior se puede dividir en tres secciones. La primera define durante cuántos segundos se asigna por defecto al cliente que lo pida una dirección IP (`default-lease-time`) antes de que tenga que realizar una petición de renovación. Esta sección también incluye una declaración del periodo máximo durante el que una máquina puede conservar una dirección IP asignada por el servidor DHCP sin realizar una petición de renovación (`max-lease-time`).

En la segunda parte se definen algunos parámetros básicos globales:

- La línea `option domain-name` define el dominio por defecto de la red.
- Mediante la entrada `option domain-name-servers`, se especifican hasta tres valores para los servidores DNS que se utilizarán para obtener los nombres de los hosts a partir de las direcciones IP y viceversa. En principio, debe configurarse un servidor de nombres en la máquina o en algún otro lugar de la red antes de configurar DHCP. El servidor de nombres también debe definir un nombre de host para cada dirección dinámica y viceversa. Para aprender cómo configurar su propio

servidor de nombres, lea el Capítulo 20, *Sistema de nombres de dominio (DNS)* (p. 397).

- La línea `option broadcast-address` define la dirección de difusión que debe utilizar el cliente solicitante.
- Mediante `option routers`, se establece dónde debe enviar el servidor los paquetes de datos que no puedan entregarse a un host de la red local (en función de las direcciones de host de origen y de destino y de la máscara de subred que se indiquen). En la mayoría de los casos, en especial en redes pequeñas, el router coincide con el gateway de Internet.
- Mediante `option subnet-mask` se especifica la máscara de red asignada a los clientes.

La última sección del archivo sirve para definir una red, incluida la máscara de subred. Para terminar, especifique el rango de direcciones que debe utilizar el daemon DHCP para asignar direcciones IP a los clientes interesados. En el Ejemplo 23.1, “El archivo de configuración /etc/dhcpd.conf” (p. 445), se puede proporcionar a los clientes cualquier dirección entre `192.168.1.10` y `192.168.1.20`, así como entre `192.168.1.100` y `192.168.1.200`.

Después de editar estas pocas líneas, debería ser posible activar el daemon DHCP mediante el comando `rcdhcpd start`. Inmediatamente estará listo para usarse. Utilice el comando `rcdhcpd check-syntax` para realizar una pequeña comprobación de la sintaxis. Si aparece cualquier problema inesperado debido a la configuración (el servidor se interrumpe con un error o no devuelve el mensaje `done` [finalizado] al iniciar) debería ser posible averiguar la causa consultando la información del registro principal del sistema `/var/log/messages` o en la consola 10 (Ctrl + Alt + F10).

En los sistemas SUSE Linux por defecto, el daemon DHCP se inicia en un entorno chroot por motivos de seguridad. Los archivos de configuración deben copiarse al entorno chroot para que el daemon pueda encontrarlos. Normalmente, no es necesario preocuparse de ello, ya que el comando `rcdhcpd start` copia los archivos automáticamente.

23.3.1 Clientes con dirección IP fija

DHCP se puede utilizar también para asignar una dirección estática predefinida a un cliente concreto. Las direcciones asignadas explícitamente siempre tienen prioridad

sobre las direcciones dinámicas del conjunto de direcciones. Además, las direcciones estáticas no caducan nunca como lo harían las direcciones dinámicas si, por ejemplo, no hubiera suficientes direcciones disponibles y el servidor necesitara redistribuirlas entre los clientes.

Para identificar a los clientes configurados con direcciones estáticas, dhcpd utiliza la dirección de hardware, que es un código global numérico, fijo y único que consta de seis pares de bytes que identifican los dispositivos de red (por ejemplo, `00:00:45:12:EE:F4`). Si se añaden al archivo de configuración del Ejemplo 23.2, "Adiciones al archivo de configuración" (p. 447) las líneas correspondientes, como las del Ejemplo 23.1, "El archivo de configuración /etc/dhcpd.conf" (p. 445), el daemon DHCP asignará siempre el mismo conjunto de datos a los clientes correspondientes.

Ejemplo 23.2 *Adiciones al archivo de configuración*

```
host earth {
hardware ethernet 00:00:45:12:EE:F4;
fixed-address 192.168.1.21;
}
```

El nombre del cliente correspondiente (`host` *`nombredelhost`*, `earth` en este caso) se introduce en la primera línea, y la dirección MAC, en la segunda. En los hosts Linux, esta dirección se puede obtener mediante el comando `ip link show` seguido del dispositivo de red (por ejemplo, `eth0`). La salida debería contener una línea de la forma

```
link/ether 00:00:45:12:EE:F4
```

En el ejemplo anterior, al cliente con la tarjeta de red de dirección MAC `00:00:45:12:EE:F4` se le asignarán automáticamente la dirección IP `192.168.1.21` y el nombre de host earth. El tipo de hardware que debe introducirse es `ethernet` en casi todos los casos, aunque también se admite `token-ring`, que suele encontrarse en sistemas IBM.

23.3.2 La versión SUSE Linux

Para mejorar la seguridad, la versión SUSE del servidor DHCP del ISC se ofrece con la revisión non-root/chroot de Ari Edelkind incluida. Esto permite que dhcpd se ejecute con el ID de usuario `nobody` y en un entorno chroot (`/var/lib/dhcp`). Para que esto sea posible, el archivo de configuración `dhcpd.conf` debe encontrarse en `/var/lib/dhcp/etc`. El guión init copia automáticamente el archivo a este directorio al iniciarse.

Se puede controlar el comportamiento del servidor respecto a esta función mediante entradas en el archivo `/etc/sysconfig/dhcpd`. Para ejecutar dhcpd sin el entorno chroot, ajuste la variable `DHCPD_RUN_CHROOTED` de `/etc/sysconfig/dhcpd` a “no”.

Para activar la resolución de nombres de host en dhcpd incluso desde el entorno chroot, es preciso copiar además otros archivos de configuración:

- `/etc/localtime`
- `/etc/host.conf`
- `/etc/hosts`
- `/etc/resolv.conf`

Estos archivos se copian en `/var/lib/dhcp/etc/` al iniciarse el guión init. Tenga en cuenta los cambios que puedan necesitar dichas copias si se modifican dinámicamente mediante guiones como `/etc/ppp/ip-up`. No obstante, no es necesario preocuparse por ello si el archivo de configuración especifica únicamente direcciones IP (en lugar de nombres de host).

Si su configuración incluye archivos adicionales que deben copiarse en el entorno chroot, especifíquelos en la variable `DHCPD_CONF_INCLUDE_FILES` del archivo `/etc/sysconfig/dhcpd`. Para garantizar que la función de registro de DHCP siga funcionando incluso después de que se reinicie el daemon syslog-ng daemon, existe una entrada adicional, `SYSLOGD_ADDITIONAL_SOCKET_DHCP`, en el archivo `/etc/sysconfig/syslog`.

23.4 Información adicional

Se puede encontrar más información sobre DHCP en el sitio Web del *Internet Software Consortium* (`http://www.isc.org/products/DHCP/`). Para obtener más información, consulte las páginas Man de `dhcpd`, `dhcpd.conf`, `dhcpd.leases` y `dhcp-options`.

24 Sincronización de la hora con NTP

El mecanismo NTP (protocolo horario de red) es un protocolo para sincronizar la hora del sistema en la red. Primero, una máquina puede obtener la hora de un servidor que sea un origen de la hora fiable. Luego, esa máquina puede a su vez actuar como origen de la hora para los demás equipos de la red. El objetivo es doble: mantener la hora absoluta y sincronizar la hora del sistema en todas las máquinas de la red.

El mantenimiento de una hora de sistema exacta es importante en muchas situaciones. El reloj de hardware integrado (BIOS) con frecuencia no cumple los requisitos de las aplicaciones como las bases de datos. La corrección manual de la hora del sistema provocaría problemas graves porque, por ejemplo, un salto hacia atrás puede provocar un mal funcionamiento de las aplicaciones importantes. En una red, normalmente es necesario sincronizar la hora del sistema en todos los equipos, pero el ajuste manual de la hora no es una buena forma de hacerlo. xntp ofrece un mecanismo para resolver estos problemas. Ajusta continuamente la hora del sistema con la ayuda de servidores horarios fiables en la red. Además habilita la gestión de los relojes de referencia locales como los relojes controlados por radio.

24.1 Configuración de un cliente NTP con YaST

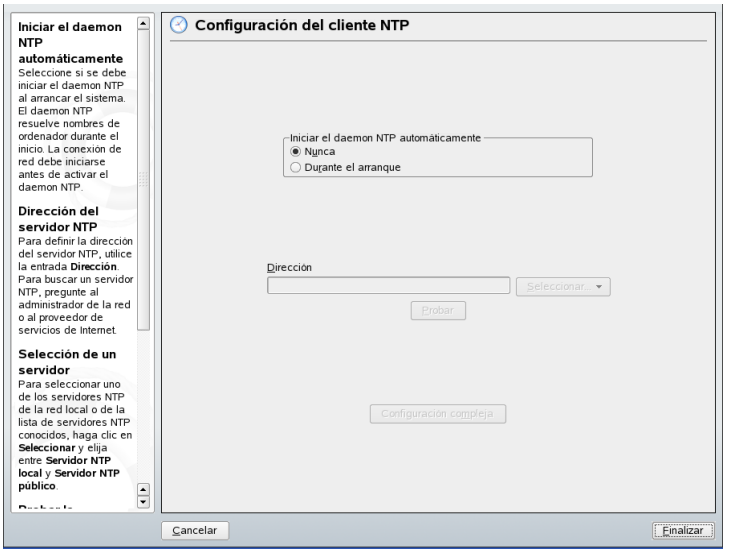
xntp está predefinido para usar el reloj del equipo local como referencia horaria. El uso del reloj del BIOS sólo sirve en el caso de que no haya disponible un origen de más precisión para consultar la hora. SUSE Linux facilita la configuración de un cliente NTP con YaST. Utilice la configuración rápida o la compleja para los clientes que no

ejecuten SuSEfirewall porque sean parte de una intranet protegida. Ambas se describen a continuación.

24.1.1 Configuración rápida del cliente NTP

La configuración sencilla del cliente NTP (*Servicios de red → Cliente NTP*) consta de dos cuadros de diálogo. En el primero, defina el modo de inicio de xntpd y el servidor al que consultar. Para iniciar xntpd automáticamente cuando el sistema arranque, haga clic en *Durante el arranque.* A continuación, especifique la *Configuración del servidor NTP.* Puede hacer clic en *Utilizar servidores aleatorios,* si no puede utilizar un servidor horario local, o bien hacer clic en *Seleccionar* para acceder a otro cuadro de diálogo donde seleccionar un servidor horario adecuado para su red.

Figura 24.1 *YaST: configuración de un cliente NTP*



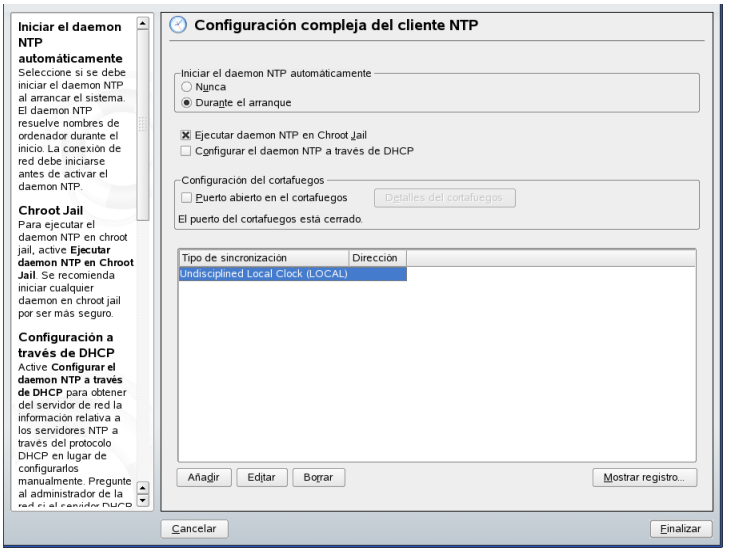
En el cuadro de diálogo de selección de servidor determine si se va a aplicar la sincronización horaria mediante un servidor horario desde la red local *(Servidor NTP local)* o un servidor horario basado en Internet que esté pendiente de la zona horaria *(Servidor NTP público).* En el caso de un servidor horario local, haga clic en *Consulta* para iniciar una consulta de SLP en busca de servidores horarios disponibles en la red. Seleccione el servidor horario más adecuado de la lista de resultados de búsqueda y salga del cuadro de diálogo con *Aceptar.* En el caso de un servidor horario público, seleccione el país

(zona horaria) y un servidor adecuado de la lista debajo de *Servidor NTP público* y, a continuación, salga del cuadro de diálogo con *Aceptar.* En el cuadro de diálogo principal, compruebe la disponibilidad del servidor seleccionado con la opción *Probar* y abandone el cuadro de diálogo con *Finalizar.*

24.1.2 configuración compleja del cliente NTP

Se puede acceder a la configuración compleja de un cliente NTP debajo de *Configuración compleja* en el cuadro de diálogo principal del módulo *Cliente NTP,* tal y como se muestra en la Figura 24.1, “YaST: configuración de un cliente NTP” (p. 450), después de seleccionar el modo de inicio tal y como se ha descrito en la configuración rápida.

Figura 24.2 *YaST: configuración compleja del cliente NTP*



En *Configuración compleja del cliente NTP,* determine si xntpd debería iniciarse en chroot jail. De esta forma se aumenta la seguridad en caso de un ataque a xntpd porque se impide que el atacante ponga en peligro todo el sistema. La opción *Configurar el daemon NTP a través de DHCP* configura el cliente NTP para que obtenga una lista de los servidores NTP disponibles en la red a través de DHCP.

Los servidores y otros orígenes horarios para las consultas del cliente se muestran en la parte inferior. Modifique esta lista según sea necesario con *Añadir, Editar* y *Suprimir*. La opción *Mostrar registro* ofrece la posibilidad de ver los archivos de registro del cliente.

Haga clic en *Añadir* para añadir un nuevo origen de información horaria. En el siguiente cuadro de diálogo, seleccione el tipo de origen con el que debería realizarse la sincronización horaria. Están disponibles las opciones siguientes:

Servidor
: Otro cuadro de diálogo le permitirá seleccionar un servidor NTP (tal y como se describe en la Sección 24.1.1, “Configuración rápida del cliente NTP” (p. 450)). Active *Usar para la sincronización inicial* para activar la sincronización de la información horaria entre el servidor y el cliente cuando arranque el sistema. Un campo de entrada permite especificar opciones adicionales para xntpd. Consulte `/usr/share/doc/packages/xntp-doc` (que forma parte del paquete `xntp-doc`) para obtener información detallada.

Par
: Un par es un equipo para el que se ha establecido una relación simétrica: actúa tanto como servidor horario como cliente. Para usar un par en la misma red en lugar de un servidor, introduzca la dirección del sistema. El resto del cuadro de diálogo es igual que el cuadro de diálogo *Servidor*.

Reloj de radio
: Para usar un reloj de radio en el sistema para la sincronización horaria, introduzca el tipo de reloj, el número de unidad, el nombre de dispositivo y otras opciones en este cuadro de diálogo. Haga clic en *Calibración del controlador* para ajustar el controlador. Hay información detallada disponible acerca de la operación del reloj de radio local en `/usr/share/doc/packages/xntp-doc/html/refclock.htm`.

Difusión saliente
: La información y las consultas horarias también pueden transmitirse mediante difusión por la red. En este cuadro de diálogo, introduzca la dirección a la que enviar tales difusiones. No active la difusión a menos que tenga un origen horario fiable como un reloj controlado por radio.

Difusión entrante
: Si desea que el cliente reciba esta información mediante difusión, escriba la dirección desde la que los paquetes respectivos deberían aceptarse en estos campos.

24.2 Configuración de xntp en la red

La manera más sencilla de usar un servidor horario en la red es definir los parámetros del servidor. Por ejemplo, si se puede llegar a un servidor horario denominado `ntp.ejemplo.com` desde la red, añada este nombre al archivo `/etc/ntp.conf`, añadiendo la línea `server ntp.ejemplo.com`. Para añadir más servidores horarios, inserte líneas adicionales con el servidor de palabras claves. Después de iniciar xntpd con el comando `rcntpd start`, se tarda aproximadamente una hora hasta que la hora se estabiliza y se crea el archivo drift para corregir el reloj del equipo local. Con este archivo, el error sistemático del reloj de hardware se puede calcular tan pronto como el equipo se encienda. La corrección se usa inmediatamente, lo que resulta en una mayor estabilidad de la hora del sistema.

Hay dos maneras posibles de usar el mecanismo NTP como un cliente. En primer lugar, el cliente puede consultar la hora desde un servidor conocido a intervalos regulares. Con muchos clientes, este enfoque puede provocar una gran carga en el servidor. En segundo lugar, el cliente puede esperar a que se envíen por la red las difusiones de NTP mediante los servidores horarios de difusión. Este enfoque tiene la desventaja de que se desconoce la calidad del servidor y un servidor que envíe información incorrecta puede provocar graves problemas.

Si la hora se obtiene mediante difusión, el nombre del servidor no es necesario. En este caso, introduzca la línea `broadcastclient` en el archivo de configuración `/etc/ntp.conf`. Para usar uno o varios servidores horarios conocidos exclusivamente, introduzca los nombres en la línea que comienza en `servers`.

24.3 Configuración de un reloj local de referencia

El paquete de software xntp contiene controladores para conectar los relojes locales de referencia. Hay disponible una lista de relojes admitidos disponibles en el archivo `/usr/share/doc/packages/xntp-doc/html/refclock.htm` del paquete

`xntp-doc`. Cada controlador está asociado con un número. En xntp, la configuración real tiene lugar mediante seudo IPs. Los relojes se introducen en el archivo `/etc/ntp.conf` como si existieran en la red. Para ello, se asignan direcciones IP especiales con la forma `127.127.t.u`. En este caso, `t` quiere decir el tipo de reloj y determina el controlador que se ha usado y la `u` se corresponde con la unidad, lo que determina la interfaz utilizada.

Normalmente, los controladores individuales tienen parámetros especiales que describen los detalles de configuración. El archivo `/usr/share/doc/packages/xntp-doc/html/driverNN.htm` (donde `NN` se corresponde con el número del controlador) ofrece información sobre el tipo concreto de reloj. Por ejemplo, el reloj "tipo 8" (reloj de radio sobre interfaz de serie) necesita un modo adicional que especifique el reloj de manera más precisa. El módulo receptor Conrad DCF77, por ejemplo, tiene el modo 5. Para usar este reloj como referencia preferida, especifique la palabra clave `prefer`. La línea `server` completa para el módulo receptor Conrad DCF77 sería:

```
server 127.127.8.0 mode 5 prefer
```

Los otros relojes siguen este mismo patrón. Después de la instalación del paquete `xntp-doc`, la documentación para xntp está disponible en el directorio `/usr/share/doc/packages/xntp-doc/html`. El archivo `/usr/share/doc/packages/xntp-doc/html/refclock.htm` ofrece enlaces a las páginas del controlador que describen los parámetros del controlador.

Servicio de directorios LDAP

25

El protocolo ligero de acceso al directorio (LDAP) es un conjunto de protocolos diseñados para acceder a los directorios de información y mantenerlos. Puede usarse LDAP con varios propósitos, como la gestión de usuarios, grupos, configuraciones del sistema y direcciones. En este capítulo se ofrece una explicación básica sobre cómo funciona OpenLDAP y cómo gestionar los datos de LDAP con YaST. Como hay varias implementaciones del protocolo LDAP, este capítulo se centra por completo en la de OpenLDAP.

En un entorno de red es fundamental mantener la información importante estructurada y disponible rápidamente. Esto puede realizarse con un servicio de directorio que, como las páginas amarillas, mantenga la información disponible con un formato de búsqueda rápido y bien estructurado.

En una situación ideal, un servidor central mantiene los datos en un directorio y los distribuye a todos los clientes mediante un protocolo concreto. Los datos se estructuran de manera que permiten que una amplia gama de aplicaciones acceda a ellos. De esta forma, no es necesario que cada herramienta de calendario o cliente de correo electrónico mantenga su propia base de datos. En lugar de ello, se puede acceder a un repositorio central. De ese modo se reduce notablemente el esfuerzo que requiere la administración de la información. El uso de un protocolo abierto y estandarizado como LDAP asegura que todas las aplicaciones cliente puedan acceder a dicha información.

Un directorio en este contexto es un tipo de base de datos optimizada para una lectura y búsqueda rápida y efectiva:

- Para hacer posible varios accesos de lectura (simultáneos), el administrador ha limitado el acceso de escritura a un pequeño número de actualizaciones. Las bases

de datos convencionales están optimizadas para aceptar el mayor volumen de datos posible en un corto espacio de tiempo.

- Puesto que los accesos de escritura sólo se pueden ejecutar de una forma restringida, se emplea un servicio de directorio para administrar sobre todo información estática que no cambia. Los datos de una base de datos convencional cambian normalmente con frecuencia (datos *dinámicos*). Los números de teléfono en un directorio de empresa no cambian tan rápidamente como, por ejemplo, las cifras manejadas en contabilidad.

- Cuando se administran datos estáticos, las actualizaciones de los conjuntos de datos existentes son escasas. Al trabajar con datos dinámicos, sobre todo en cuanto a los conjuntos de datos (cuentas bancarios o datos contables) se refiere, la coherencia de los datos es de suma importancia. Si se debe restar una cantidad de un lugar para sumarla en otro, ambas operaciones deben producirse a la vez, en una misma *transacción,* para asegurar el equilibro de los datos almacenados. Las bases de datos admiten dichas transacciones. Los directorios no. Las incoherencias de los datos por un corto período de tiempo son bastante aceptables en los directorios.

Un servicio de directorio como LDAP no está diseñado para admitir actualizaciones complejas o mecanismos de consulta. Todas las aplicaciones que accedan a este servicio deben poder hacerlo de manera rápida y sencilla.

Han existido previamente muchos servicios de directorio y aún existen en Unix y fuera de él. Novell NDS, Microsoft ADS, Street Talk de Banyan y el estándar OSI X.500 son sólo algunos ejemplos. LDAP se diseñó en un principio como una variación simplificada de DAP, el protocolo de acceso al Directorio, que se desarrolló para acceder al X.500. El estándar X.500 regula la organización jerárquica de las entradas de directorio.

LDAP es una versión más sencilla de DAP. Sin perder la jerarquía de entradas de X.500, saca partido de las posibilidades de utilizar distintas plataformas de LDAP y ahorra recursos. El uso de TCP/IP hace mucho más sencillo establecer interfaces entre una aplicación de anclaje y el servicio LDAP.

LDAP, entretanto, ha evolucionado y se utiliza cada vez más como una solución autónoma sin la ayuda de X.500. LDAP es compatible con las *referencias* con LDAPv3 (la versión del protocolo en el paquete `openldap2`), lo que permite disponer de bases de datos distribuidas. El uso de SASL (Capa sencilla de seguridad y autenticación) también es nuevo.

LDAP no está limitado a la consulta de datos de los servidores X.500, tal y como se pensó en un principio. Hay un servidor de código abierto, slapd, que puede almacenar información de objetos en una base de datos local. También hay una extensión denominada slurpd, que es la responsable de replicar varios servidores LDAP.

El paquete `openldap2` consta de lo siguiente:

slapd
: Servidor LDAPv3 autónomo que administra la información de objetos en una base de datos basada en BerkeleyDB.

slurpd
: Este programa permite la replicación de modificaciones de datos en un servidor LDAP local a otros servidores LDAP instalados en la red.

herramientas adicionales para el mantenimiento del sistema
: `slapcat`, `slapadd`, `slapindex`

25.1 LDAP frente a NIS

El administrador del sistema Unix normalmente utiliza el servicio NIS (Servicio de información de red) para la resolución de nombres y la distribución de datos por la red. Los datos de configuración incluidos en los archivos de `/etc` y los directorios `group`, `hosts`, `mail`, `netgroup`, `networks`, `passwd`, `printcap`, `protocols`, `rpc` y `services` se distribuyen por los clientes por toda la red. Estos archivos pueden mantenerse sin gran esfuerzo porque son archivos de texto sencillos. La gestión de cantidades más grandes de datos, sin embargo, se vuelve cada vez más difícil debido a una estructura inexistente. NIS está diseñado únicamente para plataformas Unix, lo que significa que no se puede utilizar como herramienta de administración de datos centralizada en redes heterogéneas.

A diferencia de NIS, el servicio LDAP no está restringido a redes Unix puras. Los servidores Windows (a partir de la versión 2000) admiten LDAP como servicio de directorio. Novell también ofrece un servicio LDAP. Las tareas de aplicaciones mencionadas anteriormente también son compatibles en sistemas que no sean Unix.

El principio de LDAP puede aplicarse a cualquier estructura de datos que deba administrarse de manera centralizada. Algunos ejemplos de su aplicación son los siguientes:

- Empleo como sustituto para el servicio NIS
- Encaminamiento de correo (postfix, sendmail)
- Libretas de direcciones para clientes de correo como Mozilla, Evolution y Outlook
- Administración de descripciones de zona para un servidor de nombres BIND9
- Autenticación de usuarios con Samba en redes heterogéneas

Esta lista puede ampliarse porque LDAP es extensible, al contrario que NIS. La estructura jerárquica claramente definida de los datos facilita la administración de grandes cantidades de ellos puesto que se puede buscar mejor.

25.2 Estructura de un árbol de directorios de LDAP

Un directorio LDAP tiene una estructura de árbol. Todas las entradas (denominadas "objetos") del directorio tienen una posición definida en esta jerarquía. Esta jerarquía se denomina *árbol de información del Directorio* (DIT). La vía completa a la entrada deseada, que la identifica de forma clara, se llama *nombre completo* o DN. Un nodo sencillo junto con la vía a esta entrada se denomina *nombre completo relativo* o RDN. Los objetos pueden asignarse generalmente a uno de dos tipos posibles:

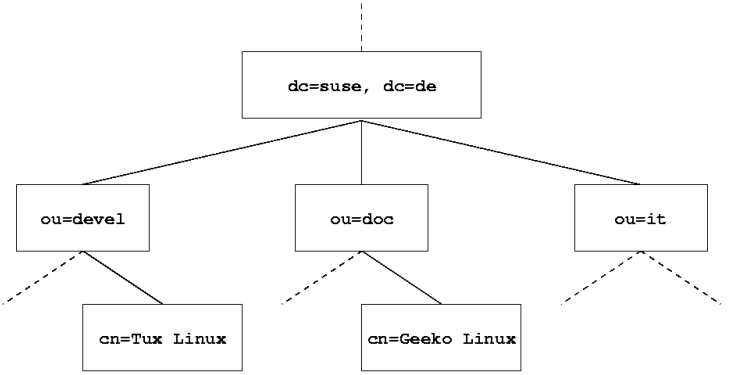
contenedor
: Estos objetos pueden a su vez contener otros objetos. Tales clases de objetos son `root` (el elemento raíz del árbol de directorios, que no existe realmente), `c` (país), `ou` (unidad organizativa) y `dc` (componente de dominio). Este modelo es comparable con los directorios (carpetas) de un sistema de archivos.

hoja
: Estos objetos se encuentran en la parte final de una rama y no incluyen objetos subordinados. Algunos ejemplos serían `person`, `InetOrgPerson` o `groupofNames`.

La parte superior de la jerarquía de directorios tiene un elemento raíz `root`. Puede contener a su vez `c` (país), `dc` (componente de dominio) o `o` (organización) como elementos subordinados. Las relaciones dentro de un árbol de directorios LDAP se

hacen más evidentes en el siguiente ejemplo, que se muestra en la Figura 25.1, “Estructura de un directorio LDAP” (p. 459).

Figura 25.1 *Estructura de un directorio LDAP*



Este diagrama completo comprende un árbol de información del Directorio ficticio. Las entradas se describen en tres niveles. Cada entrada se corresponde con un cuadro en la imagen. El *nombre completo* válido para el empleado de SUSE ficticio `Geeko Linux` en este caso es `cn=Geeko Linux,ou=doc,dc=suse,dc=de`. Se compone añadiendo el RDN `cn=Geeko Linux` al DN de la entrada precedente `ou=doc,dc=suse,dc=de`.

La determinación global de qué tipos de objetos deberían almacenarse en el DIT se realiza siguiendo un *esquema.* El tipo de objeto está determinado por la *clase del objeto.* Sirve para determinar qué atributos puede o debe asignarse el objeto en cuestión. Un esquema, por tanto, debe contener definiciones de todas las clases y atributos del objeto utilizados en el escenario de la aplicación deseada. Hay unos cuantos esquemas comunes (consulte la RFC 2252 y 2256). Sin embargo, es posible crear esquemas personalizados o usar varios esquemas que se complementen unos a otros si el entorno en el que debe operar el servidor LDAP lo necesita.

La Tabla 25.1, “Clases y atributos de objetos usados comúnmente” (p. 460) ofrece una breve descripción de las clases de objetos de `core.schema` y `inetorgperson .schema` utilizadas en el ejemplo, incluidos los atributos necesarios y los valores de atributos válidos.

Tabla 25.1 *Clases y atributos de objetos usados comúnmente*

Clase de objeto	Significado	Entrada de ejemplo	Atributos obligatorios
dcObject	*domainComponent* (componentes del nombre del dominio)	suse	dc
organizationalUnit	*organizationalUnit* (unidad organizativa)	doc	ou
inetOrgPerson	*inetOrgPerson* (datos relacionados con la persona para la intranet o Internet)	Geeko Linux	sn y cn

El Ejemplo 25.1, "Extracto de schema.core " (p. 460) muestra un extracto de una directiva de esquema con explicaciones (se han numerado las líneas para facilitar la explicación).

Ejemplo 25.1 *Extracto de schema.core*

```
#1 attributetype (2.5.4.11 NAME ( 'ou' 'organizationalUnitName')
#2        DESC 'RFC2256: unidad organizativa a la que pertenece este objeto'

#3        SUP name )

...
#4 objectclass ( 2.5.6.5 NAME 'organizationalUnit'
#5        DESC 'RFC2256: una unidad organizativa'
#6        SUP top STRUCTURAL
#7        MUST ou
#8 MAY (userPassword $ searchGuide $ seeAlso $ businessCategory
    $ x121Address $ registeredAddress $ destinationIndicator
    $ preferredDeliveryMethod $ telexNumber
    $ teletexTerminalIdentifier $ telephoneNumber
    $ internationaliSDNNumber $ facsimileTelephoneNumber
    $ street $ postOfficeBox $ postalCode $ postalAddress
    $ physicalDeliveryOfficeName
    $ st $ l $ description) )
...
```

El tipo de atributo `organizationalUnitName` y la clase de objeto correspondiente `organizationalUnit` sirven como ejemplo en este caso. La línea 1 presenta el nombre del atributo, su OID (*identificador de objeto)* único y numérico y la abreviatura del atributo.

La línea 2 ofrece una breve descripción del atributo con DESC. La RFC correspondiente en la que se basa la definición también se menciona aquí. SUP en la línea 3 indica un tipo de atributo superior al que pertenece este atributo.

La definición de la clase de objeto `organizationalUnit` comienza en la línea 4, como en la definición del atributo, con un OID y el nombre de la clase de objeto. La línea 5 presenta una breve descripción de la clase de objeto. La línea 6, con la entrada `SUP top`, indica que esta clase de objeto no está subordinada a otra. La línea 7, que comienza con MUST, muestra todos los tipos de atributos que *deben* usarse junto con un objeto del tipo `organizationalUnit`. La línea 8, que comienza con MAY, muestra todos los tipos de atributos que se permiten junto con esta clase de objeto.

Se puede encontrar una introducción muy buena sobre el uso de esquemas en la documentación de OpenLDAP. Tras la instalación, la encontrará en `/usr/share/doc/packages/openldap2/admin-guide/index.html`.

25.3 Configuración del servidor con slapd.conf

El sistema instalado contiene un archivo de configuración completo para el servidor LDAP en `/etc/openldap/slapd.conf`. Las entradas se describen brevemente y se explican los ajustes necesarios. Las entradas con una almohadilla (#) delante están inactivas. Este carácter de comentario debe eliminarse para activarlas.

25.3.1 Directivas globales en slapd.conf

Ejemplo 25.2 *slapd.conf: directiva de inclusión para esquemas*

```
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/rfc2307bis.schema
include         /etc/openldap/schema/yast.schema
```

La primera directiva de `slapd.conf`, que se muestra en el Ejemplo 25.2, “slapd.conf: directiva de inclusión para esquemas” (p. 461), especifica el esquema con el que se organiza el directorio LDAP. La entrada `core.schema` es obligatoria. Al final de

esta directiva se añaden esquemas necesarios adicionales. Puede obtener información en la documentación de OpenLDAP incluida.

Ejemplo 25.3 *slapd.conf: pidfile y argsfile*

```
pidfile /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args
```

Estos dos archivos contienen el PID (ID de proceso) y algunos de los argumentos con los que ha comenzado el proceso `slapd`. No es necesario realizar ninguna modificación aquí.

Ejemplo 25.4 *slapd.conf: Control de acceso*

```
# Sample Access Control
#       Allow read access of root DSE
# Allow self write access
#       Allow authenticated users read access
#       Allow anonymous users to authenticate
# access to dn="" by * read
  access to * by self write
              by users read
              by anonymous auth
#
# if no access controls are present, the default is:
#       Allow read by all
#
# rootdn can always write!
```

El Ejemplo 25.4, “slapd.conf: Control de acceso” (p. 462) es un extracto de `slapd.conf` que regula los permisos de acceso para el directorio LDAP en el servidor. Los ajustes que se realicen aquí en la sección global de `slapd.conf` son válidos mientras que no se declaren reglas de acceso personalizadas en la sección específica de la base de datos. Dichas reglas sobrescribirían las declaraciones globales. Tal y como se ha descrito, todos los usuarios cuentan con acceso de lectura al directorio pero sólo el administrador (`rootdn`) puede escribir en este directorio. La regulación del control de acceso en LDAP es un proceso extremadamente complejo. Las siguientes sugerencias pueden resultar útiles:

- Cada regla de acceso cuenta con la siguiente estructura:

  ```
  access to <qué> by <quién> <acceso>
  ```

- *qué* es un espacio reservado para el objeto o atributo al que se otorga acceso. Las ramas individuales del directorio se pueden proteger explícitamente con reglas independientes. También es posible procesar zonas del árbol de directorios con una

regla mediante el uso de expresiones regulares. `slapd` evalúa todas las reglas en el orden en el que se muestran en el archivo de configuración. Las reglas más generales se deberían mostrar después de las más concretas (la primera regla que `slapd` considera válida se evalúa y las entradas siguientes se omiten.

- *`quién`* determina a quién se debería otorgar acceso a las áreas determinadas con *`qué.`* Se pueden usar expresiones regulares. `slapd` aborta la evaluación de `quién` después de la primera coincidencia, de modo que las reglas más específicas deben encontrarse antes de las más generales. Las entradas que aparecen en la Tabla 25.2, "Grupos de usuarios y sus otorgamientos de acceso" (p. 463) son posibles.

Tabla 25.2 *Grupos de usuarios y sus otorgamientos de acceso*

Etiqueta	Ámbito
*	Todos los usuarios sin excepción
`anonymous`	Usuarios no autenticados ("anónimos")
`users`	Usuarios autenticados
`self`	Usuarios conectados con el objeto de destino
`dn.regex=<regex>`	Todos los usuarios que coinciden con la expresión regular

- *`acceso`* especifica el tipo de acceso. Utilice las opciones que se muestran en la Tabla 25.3, "Tipos de acceso" (p. 463).

Tabla 25.3 *Tipos de acceso*

Etiqueta	Ámbito de acceso
`none`	Sin acceso
`auth`	Para contactar con el servidor
`compare`	A objetos para acceso de comparación

Etiqueta	Ámbito de acceso
búsqueda	Para el empleo de filtros de búsqueda
read	Acceso de lectura
write	Acceso de escritura

slapd compara el derecho de acceso pedido por el cliente con los otorgados en slapd.conf. Al cliente se le otorga acceso si las reglas le permiten un derecho igual o superior al necesario. Si el cliente pide derechos superiores que los declarados en las reglas, se le denegará el acceso.

En el Ejemplo 25.5, “slapd.conf: ejemplo de control de acceso” (p. 464) se muestra un ejemplo de un control de acceso simple que puede desarrollarse de manera arbitraria mediante expresiones regulares.

Ejemplo 25.5 *slapd.conf: ejemplo de control de acceso*

```
access to  dn.regex="ou=([^,]+),dc=suse,dc=de"
by dn.regex="cn=administrator,ou=$1,dc=suse,dc=de" write
by user read
by * none
```

Esta regla indica que sólo el administrador respectivo tiene acceso de escritura a una entrada ou individual. Todos los demás usuarios autenticados tienen acceso de lectura y los demás no tienen acceso.

SUGERENCIA: Establecimiento de reglas de acceso

Si no hay una regla access to o una directiva by coincidente, se denegará el acceso. Sólo se otorgarán los derechos de acceso declarados explícitamente. Si no se declara ninguna regla en absoluto, el principio por defecto es el acceso de escritura para el administrador y de lectura para el resto.

Puede encontrar información detallada y una configuración de ejemplo correspondiente a los derechos de acceso de LDAP en la documentación en línea del paquete openldap2 instalado.

Aparte de la posibilidad de administrar los permisos de acceso con el archivo de configuración del servidor central (slapd.conf), hay información de control de

acceso (ACI). ACI permite el almacenamiento de la información de acceso para objetos individuales dentro del árbol LDAP. Este tipo de control de acceso aún no es común y los desarrolladores lo consideran todavía experimental. Consulte `http://www.openldap.org/faq/data/cache/758.html` para obtener más información.

25.3.2 Directivas específicas de base de datos en slapd.conf

Ejemplo 25.6 *slapd.conf: directivas específicas de base de datos*

```
database bdb
checkpoint      1024    5
cachesize       10000
suffix "dc=suse,dc=de"
rootdn "cn=admin,dc=suse,dc=de"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw secret
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700 recommended.
directory /var/lib/ldap
# Indices to maintain
index   objectClass     eq
```

El tipo de base de datos, una de Berkeley en este caso, está determinado en la primera línea de la sección (consulte el Ejemplo 25.6, “slapd.conf: directivas específicas de base de datos” (p. 465)). `checkpoint` determina la cantidad de datos (en kb) que se mantiene en el registro de transacciones antes de que se escriban en la base de datos real y el tiempo (en minutos) entre dos acciones de escritura. `cachesize` define el número de objetos mantenidos en el caché de la base de datos. `suffix` determina la parte del árbol de LDAP de la que el servidor es responsable. El siguiente `rootdn` determina quién posee los derechos de administrador de este servidor. El usuario que aparezca aquí no necesita tener una entrada LDAP ni existir como usuario normal. La contraseña del administrador está definida con `rootpw`. En lugar de usar aquí `secret`, es posible introducir el algoritmo hash de la contraseña del administrador creado por `slappasswd`. La directiva `directory` indica el directorio (en el sistema de archivos) en el que los directorios de la base de datos se almacenan en el servidor. La última directiva, `index objectClass eq`, da como resultado el mantenimiento de un índice en todas las clases de objetos. Los atributos que los usuarios buscan con más frecuencia pueden añadirse aquí según su uso. Las reglas personalizadas de `acceso` definidas para la base de datos se usan en lugar de las reglas globales de `acceso.`

25.3.3 Inicio y detención de los servidores

Una vez que el servidor LDAP se haya configurado completamente y realizado todas las entradas según el patrón descrito en la Sección 25.4, “Gestión de datos en el directorio LDAP” (p. 466), inicie el servidor LDAP como usuario `Root` introduciendo `rcldap start`. Para detener el servidor manualmente, introduzca el comando `rcldap stop`. Pida el estado del servidor LDAP que se esté ejecutando con `rcldap status`.

El editor de nivel de ejecución de YaST, descrito en la Sección 8.2.3, “Configuración de los servicios de sistema (nivel de ejecución) mediante YaST” (p. 204), puede usarse para que el servidor se inicie y se detenga automáticamente cuando el sistema arranque y se detenga. También es posible crear los enlaces correspondientes a los guiones de inicio y detención con el comando `insserv` desde el indicador de comandos tal y como se describe en la Sección 8.2.2, “Guiones init” (p. 200).

25.4 Gestión de datos en el directorio LDAP

OpenLDAP ofrece una serie de herramientas para la administración de datos en el directorio LDAP. Las cuatro herramientas más importantes para añadir, suprimir, buscar y modificar los datos almacenados se explican brevemente a continuación.

25.4.1 Inserción de datos en un directorio LDAP

Una vez que la configuración del servidor LDAP en `/etc/openldap/lsapd.conf` sea correcta y esté lista (presenta las entradas apropiadas para `suffix`, `directory`, `rootdn`, `rootpw` e `index`), siga con la introducción de registros. OpenLDAP cuenta con el comando `ldapadd` para esta tarea. Si es posible, añada los objetos a la base de datos en paquetes por razones prácticas. LDAP es capaz de procesar el formato LDIF (formato de intercambio de datos de LDAP) para esto. Un archivo LDIF es un archivo de texto que puede contener un número arbitrario de pares de atributo y valor. Consulte los archivos de esquema declarados en `slapd.conf` para las clases y atributos de objetos disponibles. El archivo LDIF para crear un marco general para el ejemplo

en la Figura 25.1, “Estructura de un directorio LDAP” (p. 459) tendría el aspecto del del Ejemplo 25.7, “Ejemplo de un archivo LDIF” (p. 467).

Ejemplo 25.7 *Ejemplo de un archivo LDIF*

```
# The SUSE Organization
dn: dc=suse,dc=de
objectClass: dcObject
objectClass: organization
o: SUSE AG dc: suse

# The organizational unit development (devel)
dn: ou=devel,dc=suse,dc=de
objectClass: organizationalUnit
ou: devel

# The organizational unit documentation (doc)
dn: ou=doc,dc=suse,dc=de
objectClass: organizationalUnit
ou: doc

# The organizational unit internal IT (it)
dn: ou=it,dc=suse,dc=de
objectClass: organizationalUnit
ou: it
```

IMPORTANTE: Codificación de archivos LDIF

LDAP funciona con UTF-8 (Unicode). Las diéresis deben codificarse correctamente. Utilice un editor que sea compatible con UTF-8, como Kate o versiones recientes de Emacs. De lo contrario, evite las diéresis y otro tipo de caracteres especiales o use `recode` para volver a codificar la entrada en UTF-8.

Guarde el archivo con el sufijo `.ldif` y, a continuación, trasládelo al servidor con este comando:

```
ldapadd -x -D <dn del administrador> -W -f <archivo>.ldif
```

`-x` desconecta la autenticación con SASL en este caso. `-D` indica el usuario que llama a la operación. El DN válido del administrador se introduce tal y como se ha configurado en `slapd.conf`. En el ejemplo actual, es `cn=admin,dc=suse,dc=de`. `-W` evita tener que introducir la contraseña en la línea de comando (en texto no cifrado) y activa un indicador de contraseña aparte. Esta contraseña se ha determinado previamente en `slapd.conf` con `rootpw`. `-f` traslada el nombre del archivo. Consulte los detalles de la ejecución del comando `ldapadd` en el Ejemplo 25.8, “ldapadd con ejemplo.ldif” (p. 468).

Ejemplo 25.8 *ldapadd con ejemplo.ldif*

```
ldapadd -x -D cn=admin,dc=suse,dc=de -W -f ejemplo.ldif

Enter LDAP password:
adding new entry "dc=suse,dc=de"
adding new entry "ou=devel,dc=suse,dc=de"
adding new entry "ou=doc,dc=suse,dc=de"
adding new entry "ou=it,dc=suse,dc=de"
```

Los datos de usuario de los usuarios se pueden preparar en archivos LDIF independientes. El Ejemplo 25.9, “Datos de LDIF para Tux” (p. 468) añade `Tux` al nuevo directorio LDAP.

Ejemplo 25.9 *Datos de LDIF para Tux*

```
# coworker Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
objectClass: inetOrgPerson
cn: Tux Linux
givenName: Tux
sn: Linux
mail: tux@suse.de
uid: tux
telephoneNumber: +49 1234 567-8
```

Los archivos LDIF pueden contener un número arbitrario de objetos. Es posible enviar ramas completas al servidor de una vez o sólo partes, tal y como se muestra en el ejemplo de los objetos individuales. Si es necesario modificar algunos datos con más frecuencia, se recomienda realizar una pequeña subdivisión de los objetos individuales.

25.4.2 Modificación de datos en el directorio LDAP

La herramienta `ldapmodify` sirve para modificar los datos almacenados. La manera más sencilla de hacerlo es modificar el archivo LDIF y, seguidamente, mandar el archivo modificado al servidor LDAP. Para cambiar el número de teléfono del usuario Tux de `+49 1234 567-8` a `+49 1234 567-10`, edite el archivo LDIF como en el Ejemplo 25.10, “Archivo LDIF modificado tux.ldif” (p. 469).

Ejemplo 25.10 *Archivo LDIF modificado tux.ldif*

```
# coworker Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
changetype: modify
replace: telephoneNumber
telephoneNumber: +49 1234 567-10
```

Importe el archivo modificado al directorio LDAP con el siguiente comando:

```
ldapmodify -x -D cn=admin,dc=suse,dc=de -W -f tux.ldif
```

De manera alternativa, envíe los atributos que va a cambiar directamente a `ldapmodify`. Este procedimiento se describe a continuación:

1. Inicie `ldapmodify` e introduzca la contraseña:

   ```
   ldapmodify -x -D cn=admin,dc=suse,dc=de -W
   Enter LDAP password:
   ```

2. Introduzca los cambios con cuidado teniendo en cuenta el orden de la sintaxis que se describe a continuación:

   ```
   dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
   changetype: modify
   replace: telephoneNumber
   telephoneNumber: +49 1234 567-10
   ```

Puede encontrar información detallada acerca de `ldapmodify` y la sintaxis en la página Man ldapmodify(1).

25.4.3 Búsqueda o lectura de datos desde un directorio LDAP

OpenLDAP ofrece, mediante el comando `ldapsearch`, una herramienta de línea de comando para buscar datos en un directorio LDAP y leer datos de él. Una consulta sencilla tendría la sintaxis siguiente:

```
ldapsearch -x -b dc=suse,dc=de "(objectClass=*)"
```

La opción `-b` determina la base de la búsqueda (la sección del árbol en la que debe realizarse la búsqueda). En el caso actual, es `dc=suse,dc=de`. Para realizar una búsqueda más precisa en subsecciones concretas del directorio LDAP (por ejemplo, sólo dentro del departamento `devel),` pase esta sección a `ldapsearch` con `-b`.

`-x` pide la activación de la autenticación simple. `(objectClass=*)` declara que deben leerse todos los objetos contenidos en el directorio. Esta opción de comando puede usarse tras la creación de un árbol de directorios nuevo para comprobar que se han registrado todas las entradas correctamente y que el servidor responde tal y como se desea. Puede encontrar más información sobre el uso de `ldapsearch` en la página Man correspondiente (ldapsearch(1)).

25.4.4 Supresión de datos de un directorio LDAP

Suprima las entradas no deseadas con `ldapdelete`. La sintaxis es similar a la de los comandos descritos anteriormente. Para suprimir, por ejemplo, la entrada completa de `Tux Linux`, emita el siguiente comando:

```
ldapdelete -x -D cn=admin,dc=suse,dc=de -W cn=Tux \
Linux,ou=devel,dc=suse,dc=de
```

25.5 El cliente LDAP de YaST

YaST incluye un módulo para configurar la gestión de usuarios basada en LDAP. Si no ha habilitado esta función durante la instalación, inicie el módulo seleccionando *Servicios de red → Cliente LDAP*. YaST habilitará automáticamente cualquier cambio relacionado con PAM y NSS que necesite LDAP (tal y como se describe a continuación) e instalará los archivos necesarios.

25.5.1 Procedimiento estándar

El conocimiento previo de los procesos que actúan en segundo plano de un equipo cliente le ayudará a entender cómo funciona el módulo del cliente LDAP de YaST. Si se activa LDAP para la autenticación de red o se llama al módulo YaST, se instalan los paquetes `pam_ldap` y `nss_ldap` y se adaptan los dos archivos de configuración correspondientes. `pam_ldap` es el módulo PAM responsable de la negociación entre los procesos de inicio de sesión y el directorio LDAP como origen de los datos de autenticación. El módulo dedicado `pam_ldap.so` se instala y se adapta la configuración de PAM (consulte el Ejemplo 25.11, “pam_unix2.conf adaptado a LDAP” (p. 471)).

Ejemplo 25.11 *pam_unix2.conf adaptado a LDAP*

```
auth:       use_ldap
account:    use_ldap
password:   use_ldap
session:    none
```

Al configurar manualmente los servicios adicionales para usar LDAP, incluya el módulo PAM de LDAP en el archivo de configuración PAM correspondiente al servicio en `/etc/pam.d`. Los archivos de configuración ya adaptados a los servicios individuales se pueden encontrar en `/usr/share/doc/packages/pam_ldap/pam.d/`. Copie los archivos adecuados en `/etc/pam.d`.

La resolución de nombres de `glibc` mediante el mecanismo `nsswitch` se adapta al empleo de LDAP con `nss_ldap`. Se crea un archivo `nsswitch.conf` nuevo y adaptado en `/etc/` con la instalación de este paquete. Puede obtener más información acerca del funcionamiento de `nsswitch.conf` en la Sección 18.6.1, “Archivos de configuración” (p. 381). Las líneas siguientes deben estar presentes en `nsswitch.conf` para la administración y autenticación del usuario con LDAP. Consulte el Ejemplo 25.12, “Adaptaciones en nsswitch.conf” (p. 471).

Ejemplo 25.12 *Adaptaciones en nsswitch.conf*

```
passwd: compat
group: compat

passwd_compat: ldap
group_compat: ldap
```

Estas líneas ordenan la biblioteca Resolver de `glibc` primero para evaluar los archivos correspondientes en `/etc` y después para acceder al servidor LDAP como orígenes para los datos de autenticación y de usuarios. Compruebe este mecanismo, por ejemplo, leyendo el contenido de la base de datos del usuario con el comando `getent passwd`. El conjunto devuelto debe contener un informe de los usuarios locales del sistema además de todos los usuarios almacenados en el servidor LDAP.

Para impedir que usuarios normales gestionados mediante LDAP puedan iniciar sesión en el servidor con `ssh` o `login`, los archivos `/etc/passwd` y `/etc/group` deben incluir una línea adicional. Esta es la línea `+::::::/sbin/nologin` en `/etc/passwd` y `+:::` en `/etc/group`.

25.5.2 configuración del cliente LDAP

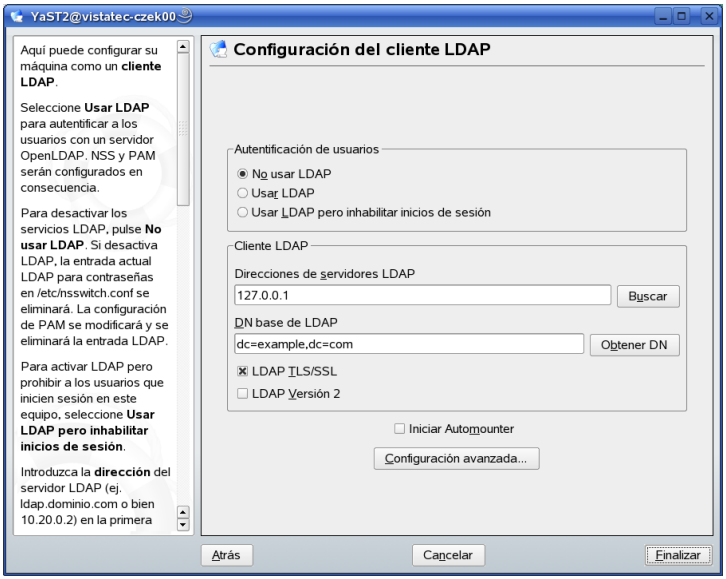
Después de que YaST se haya encargardo de los ajustes iniciales de `nss_ldap`, `pam_ldap`, `/etc/passwd` y `/etc/group`, podrá conectar sencillamente el cliente con el servidor y dejar que YaST se encargue de la gestión de usuarios mediante LDAP. La configuración básica está descrita en la "Configuración básica" (p. 472).

Utilice el cliente LDAP de YaST para seguir configurando los módulos de configuración de usuarios y grupos de YaST. Esto incluye la manipulación de los ajustes por defecto para los nuevos grupos y usuarios y el número y la naturaleza de los atributos asignados a un usuario o a un grupo. La gestión de usuarios de LDAP le permite asignar más atributos y diferentes a los usuarios y grupos que las soluciones de gestión de usuarios o grupos tradicionales. Esto se describe en la "Configuración de los módulos de administración de usuarios y grupos de YaST" (p. 476).

Configuración básica

El cuadro de diálogo de configuración básica del cliente LDAP (Figura 25.2, "YaST: configuración del cliente LDAP" (p. 473)) se abre durante la instalación si elige la gestión de usuarios de LDAP o cuando selecciona *Servicios de red* → *Cliente LDAP* en el Centro de control de YaST en el sistema instalado.

Figura 25.2 *YaST: configuración del cliente LDAP*



Para autenticar a los usuarios en el equipo con un servidor OpenLDAP y habilitar la gestión de usuarios mediante OpenLDAP, actúe de la siguiente manera:

1. Haga clic en *Usar LDAP* para habilitar la utilización de LDAP. Seleccione *Usar LDAP pero inhabilitar inicios de sesión* en su lugar si desea usar LDAP para la autenticación pero no desea que otros usuarios inicien sesión en este cliente.

2. Introduzca la dirección IP del servidor LDAP que va a usar.

3. Introduzca el *DN base de LDAP* para seleccionar la base de búsqueda en el servidor LDAP.

   Si desea que se obtenga el DN base automáticamente, haga clic en *Obtener DN*. YaST comprueba a continuación la existencia de bases de datos LDAP en la dirección de servidor especificada arriba. Elija el DN de base adecuado en los resultados de la búsqueda proporcionados por YaST.

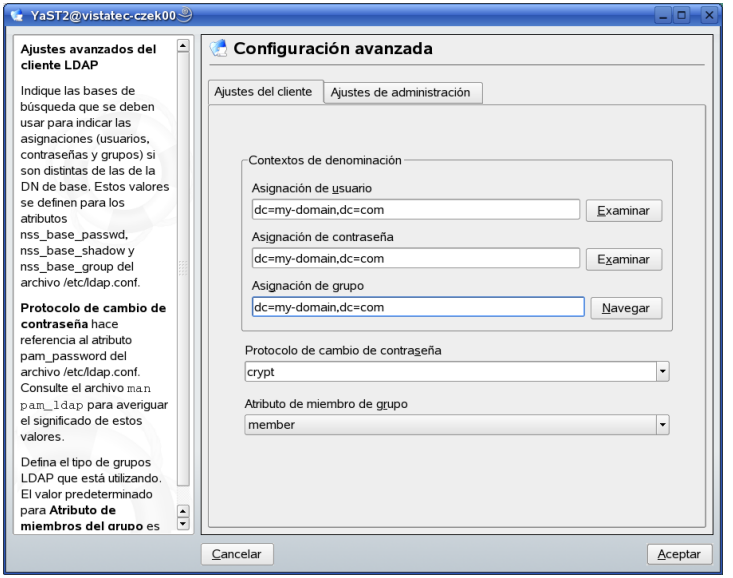
4. Si es necesario que la comunicación de TLS o SSL con el servidor esté protegida, seleccione *LDAP TLS/SSL*.

5 Si el servidor LDAP sigue usando LDAPv2, habilite explícitamente el uso de esta versión del protocolo seleccionando *LDAP versión 2.*

6 Seleccione *Iniciar Automounter* para montar los directorios remotos en el cliente, como un directorio `/home` gestionado remotamente.

7 Haga clic en *Finalizar* para aplicar los ajustes.

Figura 25.3 *YaST: Configuración avanzada*



Para modificar los datos del servidor como administrador, haga clic en *Configuración avanzada.* El siguiente cuadro de diálogo está dividido en dos pestañas. Consulte la Figura 25.3, “YaST: Configuración avanzada” (p. 474):

1 En la pestaña *Ajustes del cliente,* defina los ajustes siguientes según sus necesidades:

   a Si la base de la búsqueda de usuarios, contraseñas y grupos difiere de la base de búsqueda global especificada en *DN base de LDAP,* introduzca los distintos contextos de denominación en *Asignación de usuario, Asignación de contraseña* y *Asignación de grupo.*

b Especifique el protocolo de cambio de contraseña. El método estándar empleado siempre que se cambia una contraseña es el `cifrado`, lo que quiere decir que los algoritmos hash generados por `crypt` serán los que se usen. Para obtener más información sobre ésta y otras opciones, consulte la página Man de `pam_ldap`.

c Especifique el grupo LDAP que se va a usar con *Atributo de miembros del grupo*. El valor por defecto de esta opción es `member`.

2 En *Ajustes de administración,* defina los siguientes ajustes:

a Defina la base para el almacenamiento de los datos de gestión de usuarios mediante *Configuración de DN base*.

b Introduzca el valor adecuado para *Administrador DN*. Este DN debe ser idéntico al valor de `rootdn` especificado en `/etc/openldap/slapd.conf` para habilitar a este usuario en concreto de modo que pueda manipular los datos almacenados en el servidor LDAP. Escriba el DN completo (como `cn=admin,dc=suse,dc=de`) o active *Añadir DN base* para que el DN base se añada automáticamente al escribir `cn=admin`.

c Marque *Crear objetos de configuración predeterminada* para crear los objetos de configuración básicos en el servidor para habilitar la gestión de usuarios mediante LDAP.

d Si el equipo cliente debe actuar como servidor de archivos para directorios personales por la red, marque *Directorios personales de este equipo*.

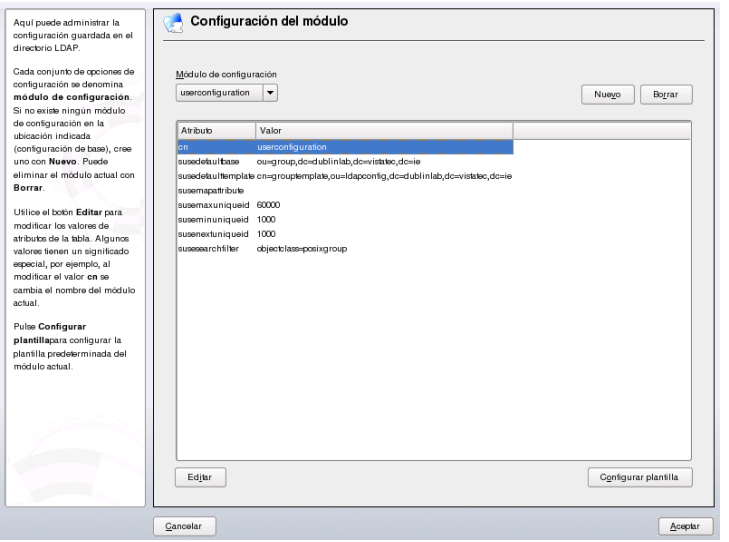
e Haga clic en *Aceptar* para dejar la *configuración avanzada* y, a continuación, en *Finalizar* para aplicar los ajustes.

Utilice *Configurar las opciones de gestión de usuarios* para editar las entradas en el servidor LDAP. Se otorgará el acceso a los módulos de configuración del servidor según las ACL y ACI almacenadas en el servidor. Siga los procedimientos descritos en "Configuración de los módulos de administración de usuarios y grupos de YaST" (p. 476).

Configuración de los módulos de administración de usuarios y grupos de YaST

Utilice el cliente LDAP de YaST para adaptar los módulos de YaST a la administración de usuarios y grupos y para ampliarlos si fuera necesario. Defina las plantillas con los valores por defecto para los atributos individuales con objeto de simplificar el registro de datos. Los ajustes predefinidos creados aquí se almacenarán como objetos LDAP en el directorio LDAP. El registro de los datos de usuario se seguirá realizando con los módulos de YaST habituales para la gestión de usuarios y grupos. Los datos registrados se almacenan como objetos LDAP en el servidor.

Figura 25.4 *YaST: configuración de módulos*



El cuadro de diálogo para la configuración de módulos (Figura 25.4, “YaST: configuración de módulos” (p. 476)) permite la creación de módulos nuevos, la selección y modificación de los módulos de configuración existentes y el diseño y la modificación de plantillas para tales módulos.

Para crear un módulo nuevo de configuración, actúe de la siguiente manera:

1. Haga clic en *Nuevo* y seleccione el tipo de módulo que crear. En el caso de un módulo de configuración de usuarios, seleccione `suseuserconfiguration` y para la configuración de grupos `susegroupconfiguration`.

2 Seleccione un nombre para la plantilla nueva.

   La vista del contenido presenta a continuación una tabla con todos los atributos permitidos en este módulo junto con los valores asignados. Aparte de todos los atributos definidos, la lista también contiene todos los atributos permitidos por el esquema actual pero que no están actualmente en uso.

3 Acepte los valores predefinidos o ajuste los valores por defecto para usarlos en la configuración de usuarios y de grupos seleccionando el atributo respectivo, pulsando *Editar* e introduciendo un valor nuevo. Cámbiele el nombre al módulo, simplemente modificando el atributo `cn`. Al hacer clic en *Suprimir* se suprime el módulo seleccionado.

4 Después de hacer clic en *Aceptar,* se añade el nuevo módulo al menú de selección.

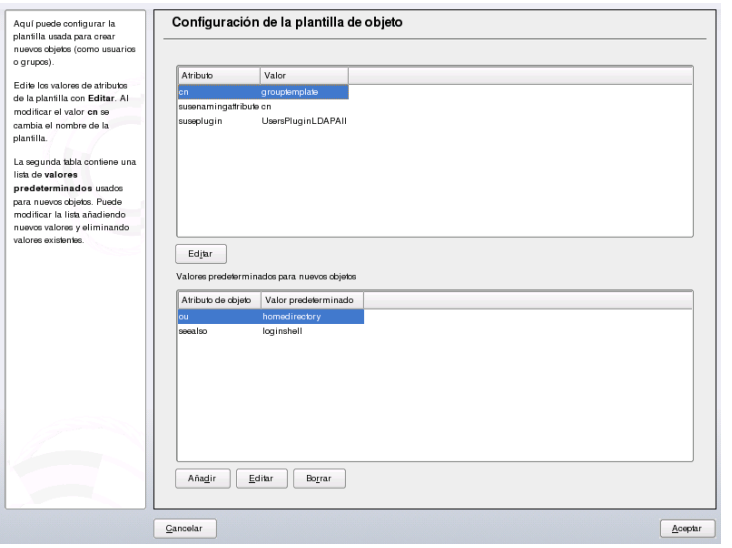
Los módulos de YaST para la administración de usuarios y grupos incrustan plantillas con valores estándar razonables. Para editar una plantilla asociada con un módulo de configuración, actúe de la siguiente manera:

1 En el cuadro de diálogo *Configuración del módulo,* haga clic en *Configurar plantilla.*

2 Determine los valores de los atributos generales asignados a esta plantilla según sus necesidades o deje algunos vacíos. Los atributos vacíos se suprimen del servidor LDAP.

3 Modifique, suprima o añada nuevos valores por defecto para los nuevos objetos (objetos de configuración de usuarios y grupos en el árbol LDAP).

Figura 25.5 *YaST: configuración de una plantilla de objeto*



Conecte la plantilla a su módulo definiendo el valor del atributo `susedefaulttemplate` del módulo en el DN de la plantilla adaptada.

SUGERENCIA

Los valores por defecto de un atributo se pueden crear a partir de otros atributos utilizando una variable en lugar de un valor absoluto. Por ejemplo, cuando se crea un usuario nuevo, `cn=%sn %givenName` se crea automáticamente a partir de los valores del atributo para `sn` y `givenName`.

Una vez que todos los módulos y plantillas se han configurado correctamente y están listos para funcionar, los nuevos grupos y usuarios se pueden registrar con YaST de la manera habitual.

25.6 Configuración de los usuarios y grupos LDAP en YaST

El registro real de los datos de usuario y de grupo difiere sólo un poco del procedimiento cuando no se usa LDAP. Las siguientes instrucciones tienen que ver con la administración de usuarios. El procedimiento para administrar grupos es análogo.

1. Acceda a la administración de usuarios de YaST mediante *Seguridad y usuarios → Administración de usuarios.*

2. Utilice *Definir filtro* para limitar la visualización de usuarios a los usuarios de LDAP e introduzca la contraseña para el DN raíz.

3. Haga clic en *Añadir* e introduzca la configuración de un usuario nuevo. Se abrirá un cuadro de diálogo con cuatro pestañas:

   a. Especifique el nombre de usuario, inicio de sesión y contraseña en la pestaña *Datos de usuario.*

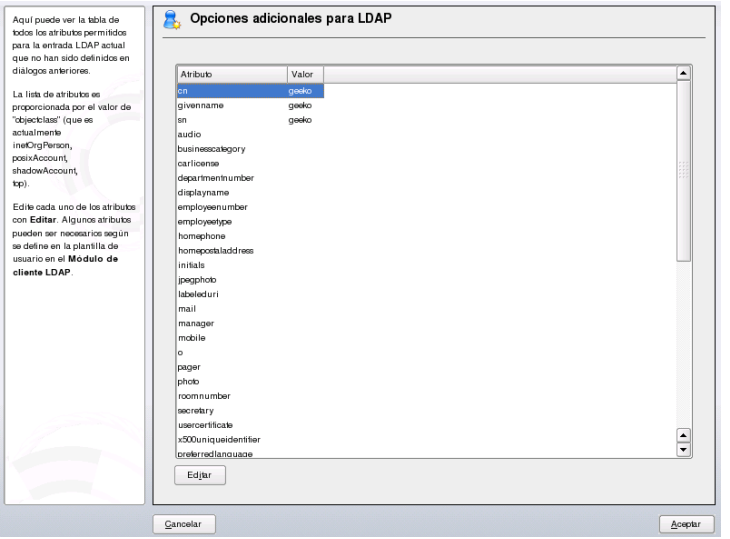
   b. Compruebe la pestaña *Detalles* para los miembros de grupo, shell de inicio de sesión y directorio personal del nuevo usuario. Si fuera necesario, cambie el valor por defecto a otros que se ajusten mejor a sus necesidades. Los valores por defecto y los ajustes de contraseña se pueden definir con el procedimiento descrito en "Configuración de los módulos de administración de usuarios y grupos de YaST" (p. 476).

   c. Modifique o acepte el valor por defecto de *Configuración de la contraseña.*

   d. Vaya a la pestaña *Plug-Ins,* seleccione el complemento LDAP y haga clic en *Ejecutar* para configurar los atributos LDAP adicionales asignados al nuevo usuario (consulte la Figura 25.6, "YaST: ajustes LDAP adicionales" (p. 480)).

4. Haga clic en *Aceptar* para aplicar los ajustes y abandonar la configuración del usuario.

Figura 25.6 *YaST: ajustes LDAP adicionales*



La forma de entrada inicial de la administración de usuarios muestra *Opciones LDAP*. De esta forma se ofrece la posibilidad de aplicar los filtros de búsqueda de LDAP al conjunto de usuarios disponible o de ir al módulo de configuración de los usuarios y grupos de LDAP seleccionando *Configuración de usuarios y grupos LDAP*.

25.7 Información adicional

Asuntos más complejos, como la configuración o establecimiento de SASL de un servidor LDAP que está replicando y que distribuye la carga de trabajo entre varios esclavos, se han omitido en este capítulo de forma intencionada. Puede encontrar información más detallada sobre ambos temas en la *OpenLDAP 2.2 Administrator's Guide* (Guía del administrador de OpenLDAP 2.2). A continuación se detallan las referencias.

El sitio Web del proyecto OpenLDAP ofrece documentación exhaustiva para usuarios LDAP principiantes y avanzados:

OpenLDAP Faq-O-Matic
: Una recopilación muy amplia de preguntas y respuestas que tienen que ver con la instalación, configuración y uso de OpenLDAP. Acceda a esta referencia desde la

siguiente dirección: http://www.openldap.org/faq/data/cache/1.html.

Quick Start Guide (Guía de inicio rápido)
: Instrucciones breves paso a paso para instalar el primer servidor LDAP. La puede encontrar en http://www.openldap.org/doc/admin22/quickstart.html o en la vía /usr/share/doc/packages/openldap2/admin-guide/quickstart.html de un sistema ya instalado.

OpenLDAP 2.2 Administrator's Guide (Guía del administrador de OpenLDAP 2.2)
: Se trata de una introducción detallada a todos los aspectos importantes de la configuración de LDAP, lo que incluye los controles de acceso y el cifrado. Consulte http://www.openldap.org/doc/admin22/ o, en un sistema instalado, acceda a /usr/share/doc/packages/openldap2/admin-guide/index.html.

Introducción a LDAP
: Se trata de una introducción general detallada de los principios básicos de LDAP: http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf.

Documentación impresa sobre LDAP:

- *LDAP System Administration* (Administración del sistema LDAP) escrito por Gerald Carter (ISBN 1-56592-491-6)

- *Understanding and Deploying LDAP Directory Services* (Comprensión e implantación de los servicios de directorio de LDAP) escrito por Howes, Smith y Good (ISBN 0-672-32316-8)

El material de referencia más reciente sobre LDAP son las RFC (petición de comentarios) 2251 a 2256.

26 Servidor HTTP Apache

Con una cuota de mercado superior al 70%, el servidor HTTP Apache (Apache) es el servidor Web más utilizado del mundo, según la encuesta de noviembre de 2005 de http://www.netcraft.com/. Apache, desarrollado por Apache Software Foundation (http://www.apache.org/), está disponible para la mayoría de sistemas operativos. SUSE Linux incluye la versión 2.2 de Apache. En este capítulo aprenderá a instalar y configurar un servidor Web, a utilizar SSL, CGI y módulos adicionales, así como a resolver problemas relacionados con Apache.

26.1 Inicio rápido

Con la ayuda de esta sección, podrá iniciar y configurar Apache rápidamente. Debe ser un usuario `Root` para poder instalar y configurar Apache.

26.1.1 Requisitos

Asegúrese de que se cumplen los siguientes requisitos antes de configurar el servidor Web Apache:

1. La red del equipo está configurada correctamente. Para obtener más información acerca de este tema, consulte el Capítulo 18, *Trabajo en red básico* (p. 345).

2. La hora exacta del sistema del equipo se mantiene gracias a la sincronización con un servidor horario, lo que es preciso debido a que ciertas partes del protocolo HTTP dependen de que la hora sea correcta. Consulte el Capítulo 24, *Sincroni-*

zación de la hora con NTP (p. 449) para obtener más información acerca de este tema.

3. Están instaladas las últimas actualizaciones de seguridad. Si no está seguro, ejecute una actualización en línea de YaST.

4. El puerto de servidor Web por defecto (puerto 80) está abierto en el cortafuegos. Para ello, configure SUSEFirewall2 para que se permita el servicio *Servidor HTTP* en la zona externa, lo que puede hacerse utilizando YaST. Encontrará información detallada en "Configuración con YaST" (p. 116).

26.1.2 Instalación

Apache no se instala por defecto en SUSE Linux. Para instalarlo, inicie YaST y seleccione *Software → Instalar/desinstalar software.* A continuación, elija *Filtro → Selecciones* y después seleccione *Servidor Web sencillo con Apache2.* Confirme la instalación de los paquetes dependientes para finalizar el proceso de instalación.

Apache se instala con una configuración estándar predefinida que se ejecuta sin necesidad de realizar acciones adicionales. La instalación incluye el módulo de multiprocesamiento `apache2-prefork`, así como el módulo PHP5. Consulte la Sección 26.4, "Instalación, activación y configuración de módulos" (p. 502) para obtener más información sobre los módulos.

26.1.3 Iniciar

Para iniciar Apache y asegurarse de que se inicia automáticamente durante el arranque, inicie YaST y seleccione *Sistema → Editor de niveles de ejecución.* Busque *apache2* y elija *Habilitar* el servicio. El servidor Web se iniciará inmediatamente. Cuando guarde los cambios mediante *Finalizar,* el sistema estará configurado para iniciar Apache automáticamente en los niveles de ejecución 3 y 5 durante el arranque. Para obtener más información acerca de los niveles de ejecución en SUSE Linux y una descripción del editor del nivel de ejecución de YaST, consulte la Sección 8.2.3, "Configuración de los servicios de sistema (nivel de ejecución) mediante YaST" (p. 204).

Para iniciar Apache desde la shell, ejecute `rcapache2 start`. Para asegurarse de que Apache se inicia automáticamente durante el arranque en los niveles de ejecución 3 y 5, utilice `chkconfig -a apache2`.

Si no ha recibido mensajes de error al iniciar Apache, el servidor Web debería ejecutarse normalmente. Inicie un navegador y abra `http://localhost/`. Debería ver una página de prueba de Apache que comienza con el texto "If you can see this, it means that the installation of the Apache Web server software on this system was successful." (Si ve esta página, significa que la instalación del software del servidor Web Apache en el sistema se ha realizado correctamente). Si no ve esa página, consulte la Sección 26.8, "Solución de problemas" (p. 522).

Una vez que el servidor Web se esté ejecutando, podrá añadir documentos propios, ajustar la configuración según sus necesidades o añadir distintas funcionalidades mediante la instalación de módulos.

26.2 Configuración de Apache

Apache se puede configurar en SUSE Linux de dos modos diferentes: con YaST o manualmente. La configuración manual ofrece un nivel superior de detalle, pero carece de la comodidad de la interfaz gráfica de YaST.

IMPORTANTE: Cambios de configuración

Los cambios que se realizan en la mayoría de los valores de configuración de Apache sólo surten efecto después de reiniciar Apache. Esto sucede automáticamente cuando se utiliza YaST y se termina la configuración con la opción *Activado* seleccionada para el servicio HTTP. El reinicio manual se describe en la Sección 26.3, "Inicio y detención de Apache" (p. 500). La mayoría de los cambios de configuración sólo requieren volver a cargar el programa con `rcapache2 reload`.

26.2.1 Configuración manual de Apache

Configurar Apache manualmente implica editar archivos de configuración de sólo texto como usuario `Root`.

Archivos de configuración

Los archivos de configuración de Apache se pueden encontrar en dos ubicaciones distintas:

- `/etc/sysconfig/apache2`
- `/etc/apache2/`

`/etc/sysconfig/apache2`

`/etc/sysconfig/apache2` controla algunos de los ajustes globales de Apache, como los módulos que se van a cargar, los archivos de configuración adicionales que se deben incluir, los indicadores con los que debe iniciarse el servidor y los indicadores que deben añadirse a la línea de comandos. Todas las opciones de configuración de este archivo están ampliamente documentadas, por lo que no se mencionan aquí. En el caso de servidores Web de uso general, los ajustes de `/etc/sysconfig/apache2` deberían ser suficientes para cualquier necesidad de configuración.

IMPORTANTE: ya no hay módulo SuSEconfig para Apache

El módulo SuSEconfig para Apache se ha eliminado de SUSE Linux, pues ya no es necesario para ejecutar `SuSEconfig` tras cambiar `/etc/sysconfig/apache2`.

`/etc/apache2/`

`/etc/apache2/` incluye todos los archivos de configuración de Apache. A continuación se explica la finalidad de cada archivo. Cada archivo incluye varias opciones de configuración (a las que también se hace referencia como *directivas*). Todas las opciones de configuración de estos archivos están ampliamente documentadas, por lo que no se mencionan aquí.

Los archivos de configuración de Apache están organizados del siguiente modo:

```
/etc/apache2/
 |
 |- charset.conv
 |- conf.d/
 |   |
 |   |- *.conf
 |
```

```
|- default-server.conf
|- errors.conf
|- httpd.conf
|- listen.conf
|- magic
|- mime.types
|- mod_*.conf
|- server-tuning.conf
|- ssl-global.conf
|- ssl.*
|- sysconfig.d
|   |
|   |- global.conf
|   |- include.conf
|   |- loadmodule.conf . .
|
|- uid.conf
|- vhosts.d
|   |- *.conf
```

Archivos de configuración de Apache en /etc/apache2/

`charset.conv`
: Especifica los conjuntos de caracteres que se deben utilizar para los distintos idiomas. No se debe editar.

`conf.d/*.conf`
: Archivos de configuración añadidos por otros módulos. Estos archivos se pueden incluir en la configuración de hosts virtuales cuando sea preciso. Consulte `vhosts.d/vhost.template` para ver ejemplos. Con ellos, se pueden proporcionar distintos conjuntos de módulos para hosts virtuales diferentes.

`default-server.conf`
: Configuración global para todos los hosts virtuales con valores por defecto adecuados. En lugar de cambiar los valores, sobrescríbalos con una configuración de host virtual.

`errors.conf`
: Define el modo en que Apache responde a los errores. Para personalizar estos mensajes para todos los hosts virtuales, edite este archivo. O bien, sobrescriba estas directivas en las configuraciones de hosts virtuales.

`httpd.conf`
: Archivo de configuración del servidor Apache principal. Evite modificar este archivo. Está integrado principalmente por declaraciones y ajustes globales.

Sobrescriba los ajustes globales en los archivos de configuración correspondientes incluidos en esta lista. Cambie los ajustes específicos de cada host (como la raíz de documentos) en la configuración de host virtual.

`listen.conf`
: Enlaza Apache con direcciones IP y puertos específicos. Los hosts virtuales basados en nombres (consulte "Hosts virtuales basados en nombres" (p. 490)) también se configuran aquí.

`magic`
: Datos para el módulo mime_magic que permiten que Apache determine automáticamente el tipo MIME de los archivos desconocidos. No se debe modificar.

`mime.types`
: Tipos MIME reconocidos por el sistema (en realidad, se trata de un enlace a `/etc/mime.types`). No se debe editar. Si necesita añadir tipos MIME que no estén incluidos, añádalos a `mod_mime-defaults.conf`.

`mod_*.conf`
: Archivos de configuración para los módulos que se instalan por defecto. Consulte la Sección 26.4, "Instalación, activación y configuración de módulos" (p. 502) para obtener información detallada. Tenga en cuenta que los archivos de configuración para módulos opcionales se encuentran en el directorio `conf.d`.

`server-tuning.conf`
: Incluye directivas de configuración para los distintos módulos de multiprocesamiento o MPM (consulte la Sección 26.4.4, "Módulos de multiprocesamiento" (p. 507)), así como opciones de configuración generales que controlan el rendimiento de Apache. Pruebe adecuadamente el servidor Web cuando modifique este archivo.

`ssl-global.conf` y `ssl.*`
: Configuración de SSL global y datos de certificado SSL. Consulte la Sección 26.6, "Configuración de un servidor Web seguro con SSL" (p. 513) para obtener información detallada.

`sysconfig.d/*.conf`
: Archivos de configuración generados automáticamente desde `/etc/sysconfig/apache2`. No cambie ninguno de estos archivos; en su lugar, modifique `/etc/sysconfig/apache2`. No coloque ningún otro archivo de configuración en este directorio.

`uid.conf`
: Especifica los ID de usuario y de grupo bajo los que se ejecuta Apache. No se debe modificar.

`vhosts.d/*.conf`
: Aquí debe encontrarse la configuración de hosts virtuales. El directorio incluye archivos de plantilla para hosts virtuales con o sin SSL. Cada archivo de este directorio que termine en `.conf` se incluye automáticamente en la configuración de Apache. Consulte "Configuración de hosts virtuales" (p. 489) para obtener información detallada.

Configuración de hosts virtuales

El término *host virtual* hace referencia a la capacidad de Apache para proporcionar servicio a varios identificadores de recursos universales (URI, del inglés Universal Resource Identifiers) desde el mismo equipo físico. Esto significa que varios dominios, como www.ejemplo.com y www.ejemplo.net pueden ejecutarse desde un mismo servidor Web en un equipo físico.

Es una costumbre habitual emplear hosts virtuales para ahorrar esfuerzos administrativos (sólo es necesario realizar el mantenimiento de un servidor Web) y gastos de hardware (no es necesario emplear un servidor dedicado para cada dominio). Los hosts virtuales pueden estar basados en nombres, en IP o en puertos.

Los hosts virtuales se pueden configurar mediante YaST (consulte "Hosts virtuales" (p. 497)) o bien editando manualmente un archivo de configuración. Apache está preparado para emplear por defecto en SUSE Linux un archivo de configuración por cada host virtual `/etc/apache2/vhosts.d/`. Todos los archivos que tengan la extensión `.conf` se incluirán automáticamente en la configuración. En este directorio se proporciona una plantilla básica para un host virtual (`vhost.template` o `vhost-ssl.template` para un host virtual con compatibilidad para SSL).

SUGERENCIA: cree siempre una configuración de host virtual

Se recomienda crear siempre un archivo de configuración de host virtual, incluso cuando el servidor Web albergue un solo dominio. Con ello, no sólo se tiene la configuración específica del dominio en un archivo, sino que se puede recuperar en cualquier momento una configuración básica de trabajo con sólo mover, suprimir o renombrar el archivo de configuración del host

virtual. Por la misma razón, debe siempre crear archivos de configuración independientes para cada host virtual.

El bloque `<VirtualHost></VirtualHost>` incluye la información que se aplica a un dominio concreto. Cuando Apache recibe una petición de un cliente relacionada con un host virtual definido, emplea las directivas incluidas en esta sección. Casi todas las directivas se pueden utilizar en un contexto de host virtual. Consulte `http://httpd.apache.org/docs/2.0/mod/quickreference.html` para obtener más información acerca de las directivas de configuración de Apache.

Hosts virtuales basados en nombres

Los hosts virtuales basados en nombres permiten que más de un sitio Web proporcione servicios desde una misma dirección IP. Apache utiliza el campo de host en el encabezado HTTP enviado por el cliente para conectar la petición con una entrada `ServerName` (Nombre del servidor) que coincida en una de las declaraciones de host virtuales. Si no se encuentra ninguna entrada `ServerName` coincidente, se utiliza por defecto la primera entrada de host virtual que se especifique.

La directiva `NameVirtualHost` (Nombre del host virtual) indica a Apache la dirección IP y, opcionalmente, el puerto en los que debe escuchar las peticiones de los clientes que contengan el nombre del dominio en el encabezado HTTP. Esta opción se configura en el archivo `/etc/apache2/listen.conf`.

El primer argumento puede ser un nombre completo de dominio, pero es recomendable utilizar la dirección IP. El segundo argumento es opcional y corresponde al puerto. Por defecto, el puerto 80 se utiliza y se configura mediante la directiva `Listen` (Escucha).

El comodín `*` puede utilizarse tanto para la dirección IP como para el número de puerto, a fin de recibir peticiones en todas las interfaces. Las direcciones IPv6 deben incluirse entre corchetes.

Ejemplo 26.1 *Variaciones de entradas VirtualHost basadas en nombres*

```
# NameVirtualHost Dirección IP[:puerto] NameVirtualHost 192.168.1.100:80
NameVirtualHost 192.168.1.100
NameVirtualHost *:80
NameVirtualHost *
NameVirtualHost [2002:c0a8:164::]:80
```

La etiqueta de apertura `VirtualHost` (Host virtual) indica la dirección IP (o el nombre completo del dominio) que se haya declarado previamente mediante

`NameVirtualHost` (Nombre del host virtual) como argumento en una configuración de host virtual basada en nombres. El número de puerto declarado anteriormente con la directiva `NameVirtualHost` es opcional.

También está permitido utilizar el comodín `*` como sustituto de la dirección IP. Esta sintaxis sólo es válida en combinación con el uso de comodines en `NameVirtualHost *`. Las direcciones IPv6 deben estar incluidas entre corchetes.

Ejemplo 26.2 *Directivas VirtualHost basadas en nombres*

```
<VirtualHost 192.168.1.100:80>
  ...
</VirtualHost>

<VirtualHost 192.168.1.100>
  ...
</VirtualHost>

<VirtualHost *:80>
  ...
</VirtualHost>

<VirtualHost *>
  ...
</VirtualHost>

<VirtualHost [2002:c0a8:164::]>
  ...
</VirtualHost>
```

Hosts virtuales basados en IP

Esta configuración alternativa de host virtual requiere la configuración de varias direcciones IP para un mismo equipo. Una instancia de Apache aloja varios dominios y a cada uno de ellos se le asigna una dirección IP diferente.

El servidor físico debe disponer de una dirección IP para cada host virtual basado en IP. Si el equipo no tiene varias tarjetas de red, también se pueden emplear interfaces de red virtuales (asignación de alias IP).

El siguiente ejemplo muestra un servidor Apache que se ejecuta en un equipo con la dirección IP `192.168.0.10` y aloja dos dominios en las direcciones IP adicionales `192.168.0.20` y `192.168.0.30`. Debe emplearse un bloque `VirtualHost` para cada uno de los servidores virtuales.

Ejemplo 26.3 *Directivas VirtualHost basadas en IP*

```
<VirtualHost 192.168.0.20>
  ...
</VirtualHost>

<VirtualHost 192.168.0.30>
  ...
</VirtualHost>
```

En este ejemplo, las directivas `VirtualHost` sólo se especifican para las interfaces distintas de `192.168.0.10`. Cuando se configura una directiva `Listen` también para `192.168.0.10`, se debe crear un host virtual basado en IP independiente para que responda a las peticiones HTTP de esa interfaz; de lo contrario, se aplican las directivas incluidas en el archivo de configuración de servidor por defecto (`/etc/apache2/default-server.conf`).

Configuración básica de host virtual

Al menos las siguientes directivas deben estar presentes en cada configuración de host virtual para configurar un host virtual. Consulte `/etc/apache2/vhosts.d/vhost.template` para conocer más opciones.

`ServerName`
: Nombre completo del dominio bajo el cual se encuentra el host.

`DocumentRoot`
: Vía al directorio desde el cual Apache debe proporcionar archivos para este host. Por razones de seguridad, el acceso al sistema de archivos completo está prohibido por defecto, por lo que se debe desbloquear este directorio específicamente dentro de un contenedor `Directorio.`

`ServerAdmin`
: Dirección de correo electrónico del administrador del servidor. Esta dirección se muestra, por ejemplo, en las páginas de errores que crea Apache.

`ErrorLog`
: Archivo de registro de errores de este host virtual. Aunque no es preciso crear archivos de registro de errores independientes para cada host virtual, suele hacerse por lo general debido a que facilita la depuración de los errores. `/var/log/apache2/` es el directorio por defecto donde deben guardarse los archivos de registro de Apache.

`CustomLog`
: Archivo de registro de acceso de este host virtual. Aunque no es preciso crear archivos de registro de acceso independientes para cada host virtual, suele hacerse por lo general debido a que facilita el análisis de las estadísticas de acceso de cada host. `/var/log/apache2/` es el directorio por defecto donde deben guardarse los archivos de registro de Apache.

Como ya se ha dicho, el acceso al sistema de archivos completo está prohibido por defecto por razones de seguridad. Por lo tanto, debe desbloquear explícitamente el directorio `DocumentRoot` en el que haya colocado los archivos que debe proporcionar Apache:

```
<Directory "/srv/www/example.com_htdocs">
  Order allow,deny
  Allow from all
</Directory>
```

El archivo de configuración completo tiene el aspecto siguiente:

Ejemplo 26.4 *Configuración básica de VirtualHost*

```
<VirtualHost 192.168.0.10>
  ServerName www.example.com
  DocumentRoot /srv/www/example.com_htdocs
  ServerAdmin webmaster@example.com
  ErrorLog /var/log/apache2/www.example.com_log
  CustomLog /var/log/apache2/www.example.com-access_log common
  <Directory "/srv/www/example.com">
    Order allow,deny
    Allow from all
  </Directory>
</VirtualHost>
```

26.2.2 Configuración de Apache con YaST

Para configurar el servidor Web con YaST, inicie YaST y seleccione *Servicios de red → Servidor HTTP*. Cuando se inicia el módulo por primera vez, se inicia el `Asistente del servidor HTTP`, que le solicitará que tome algunas decisiones básicas relativas a la administración del servidor. Una vez que finalice el asistente, se mostrará el cuadro de diálogo descrito en “Configuración del servidor HTTP” (p. 498) cada vez que llame al módulo *Servidor HTTP Server*.

Asistente de servidor HTTP

El Asistente del servidor HTTP consta de cinco pasos. En el último paso del cuadro de diálogo, podrá introducir el modo de configuración avanzada para realizar ajustes aún más específicos.

Selección de dispositivos de red

Especifique las interfaces y los puertos de red que Apache utilizará para escuchar las peticiones entrantes. Puede seleccionar cualquier combinación de las interfaces de red existentes y sus direcciones IP respectivas. Es posible utilizar productos de los tres rangos (puertos conocidos, puertos registrados y puertos dinámicos o privados) no reservados por otros servicios. El ajuste por defecto es escuchar en todas las interfaces de red (direcciones IP) del puerto 80.

Seleccione *Open Firewall for Selected Ports* (Abrir cortafuegos para los puertos seleccionados) para abrir los puertos en el cortafuegos en el que escucha el servidor Web. Este paso es necesario para que el servidor Web esté disponible en la red, que puede ser una LAN, una WAN o Internet. Mantener el puerto de escucha cerrado es útil únicamente en situaciones de prueba en las que no es necesario el acceso externo al servidor Web.

Haga clic en *Siguiente* para continuar.

Módulos

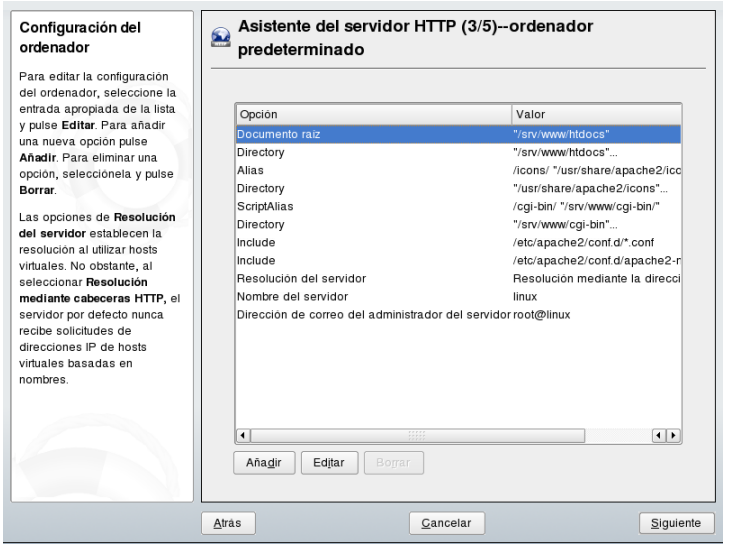
La opción de configuración *Módulos* permite la activación o desactivación de los idiomas de guión que debe admitir el servidor Web. En relación con la activación o desactivación de otros módulos, consulte "Módulos del servidor" (p. 500). Haga clic en *Siguiente* para acceder al siguiente cuadro de diálogo.

Ordenador predeterminado

Esta opción pertenece al servidor Web por defecto. Como se explica en "Configuración de hosts virtuales" (p. 489), Apache puede servir a varios hosts virtuales desde una sola máquina. El primer host virtual declarado en el archivo de configuración se conoce normalmente como *host por defecto* (u ordenador predeterminado). Cada uno de los hosts virtuales hereda la configuración de host del equipo por defecto.

Para editar los ajustes del host (también llamados *directivas*), seleccione la entrada apropiada en la tabla y haga clic en *Editar*. Para añadir directivas nuevas, haga clic en *Añadir*. Para eliminar una directiva, selecciónela y haga clic en *Suprimir*.

Figura 26.1 *Asistente de servidor HTTP: Ordenador predeterminado*



A continuación, se ofrece una lista con los ajustes por defecto del servidor:

`Raíz de documentos`
: Vía al directorio desde el cual Apache proporciona archivos para este host. `/srv/www/htdocs` es la ubicación por defecto.

`Alias`
: Con la ayuda de las directivas `Alias`, las URL se pueden asignar a ubicaciones físicas de sistemas de archivos. Esto significa que es posible acceder a una vía determinada incluso si se encuentra fuera del `Documento raíz` del sistema de archivos mediante una URL con el alias de esa vía.

  Los `Alias /iconos` SUSE Linux por defecto señalan `/usr/share/apache2/icons` para los iconos de Apache que aparecen en la vista de índice del directorio.

`ScriptAlias`
: Al igual que la directiva `Alias`, la directiva `ScriptAlias` asigna una URL a la ubicación de un sistema de archivos. La diferencia es que `ScriptAlias` designa el directorio destino como ubicación CGI, lo que significa que los guiones CGI deberían ejecutarse en dicha ubicación.

`Directorio`
: Con el ajuste `Directorio,` puede establecer un grupo de opciones de configuración que se aplicarán únicamente al directorio especificado.

  Aquí se configuran las opciones de acceso y de visualización para los directorios `/usr/share/apache2/icons` y `/srv/www/cgi-bin`. No debería ser preciso modificar los valores por defecto.

`Include`
: Con esta directiva se pueden especificar archivos de configuración adicionales. `/etc/apache2/conf.d/*.conf` es el directorio que contiene los archivos de configuración que se incluyen en módulos externos. Por defecto se incluyen todos los archivos de este directorio (`*.conf`). `/etc/apache2/conf.d/apache2-manual?conf` es el directorio que contiene los archivos de configuración `apache2-manual`.

`Nombre del servidor`
: Éste especifica la URL por defecto que utilizan los clientes para ponerse en contacto con el servidor Web. Utilice un nombre completo de dominio (NCD) para acceder al servidor Web en `http://`*`NCD/`* o la dirección IP correspondiente. No se puede elegir aquí un nombre arbitrario, ya que se debe "reconocer" el nombre del servidor.

`Correo electrónico del administrador de servidores`
: Dirección de correo electrónico del administrador del servidor. Esta dirección se muestra, por ejemplo, en las páginas de errores que crea Apache.

`Resolución del servidor`
: Esta opción hace referencia a "Configuración de hosts virtuales" (p. 489). *Determine Request Server by HTTP Headers* (Determinar servidor de peticiones por encabezados HTTP) ofrece una respuesta por parte de `VirtualHost` a una petición realizada a su nombre de servidor (consulte "Hosts virtuales basados en nombres" (p. 490)). *Determine Request Server by Server IP Address* (Determinar servidor de peticiones por dirección IP del servidor) hace que Apache seleccione el host solicitado por la información de encabezados HTTP que envía el cliente. Consulte

"Hosts virtuales basados en IP" (p. 491) para obtener más información acerca de los hosts virtuales basados en IP.

Una vez que haya terminado con el paso *Ordenador predeterminado,* haga clic en *Siguiente* para continuar con la configuración.

Hosts virtuales

En este paso, el asistente muestra una lista de los hosts virtuales ya configurados (consulte "Configuración de hosts virtuales" (p. 489)). Si no ha realizado cambios manuales antes de iniciar el asistente HTTP de YaST, sólo se mostrará un host virtual, idéntico al host por defecto configurado en el paso anterior. Este host estará marcado como opción por defecto mediante un asterisco colocado junto al nombre del servidor.

Para añadir un host, haga clic en *Añadir* y aparecerá un cuadro de diálogo en el que introducir información básica acerca del host. *Identificación del servidor* incluye el nombre del servidor, la raíz del contenido del servidor (`DocumentRoot`) y el correo electrónico del administrador. La opción *Resolución del servidor* se utiliza para determinar cómo se identifica un host (mediante el nombre o la IP). Estas opciones se explican en "Ordenador predeterminado" (p. 494).

Si hace clic en *Siguiente,* accederá a la segunda parte del cuadro de diálogo de configuración del host virtual.

En esta segunda parte puede especificar si quiere habilitar guiones CGI y el directorio que se debe utilizar para esos guiones. También puede habilitar SSL. Si lo hace, debe especificar además la vía al certificado. Consulte la Sección 26.6.2, "Configuración de Apache con SSL" (p. 518) para obtener información detallada acerca de SSL y de los certificados. Con la opción *Índice de directorio,* puede especificar el archivo que se debe mostrar cuando el cliente solicita un directorio (index.html por defecto). Puede añadir uno o varios nombres de archivo (separados por espacios) si quiere cambiar la configuración por defecto. Con *Habilitar HTML público,* el contenido de los directorios públicos de los usuarios (`~usuario/public_html/`) pasa a estar disponible en el servidor en `http://www.ejemplo.com/~usuario`.

IMPORTANTE: Creación de hosts virtuales

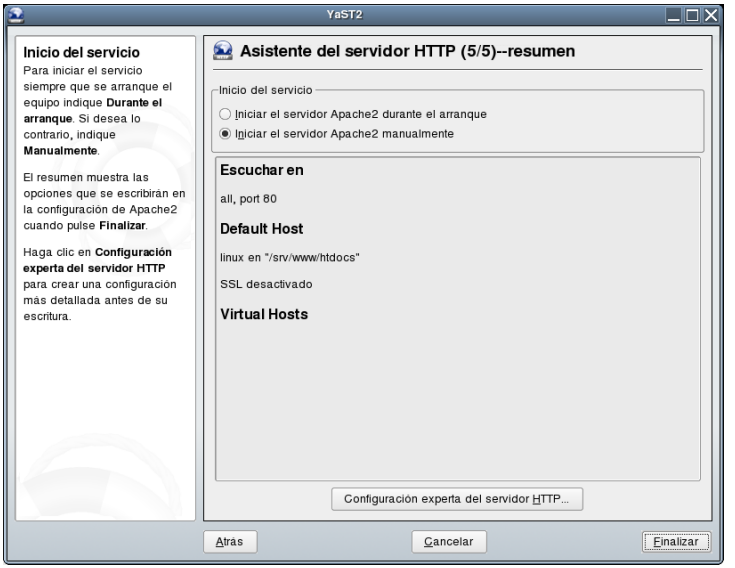
No es posible añadir hosts virtuales a voluntad. Si se utilizan hosts virtuales basados en nombres, cada nombre se debe resolver en la red. Si se utilizan

hosts virtuales basados en direcciones IP, sólo se puede asignar un host a cada dirección IP disponible.

Resumen

Éste es el paso final del asistente. Determine cómo y cuándo se inicia el servidor Apache: al arrancar o de forma manual. Consulte también un breve resumen de la configuración definida hasta el momento. Si está satisfecho con la configuración, haga clic en *Finalizar* para terminar la configuración. Si quiere cambiar algún ajuste, haga clic en *Atrás* hasta que acceda al cuadro de diálogo oportuno. Si hace clic en *Configuración experta del servidor HTTP,* se abrirá el cuadro de diálogo que se describe en "Configuración del servidor HTTP" (p. 498).

Figura 26.2 *Asistente de servidor HTTP: Resumen*



Configuración del servidor HTTP

El cuadro de diálogo *Configuración del servidor HTTP* le permite además realizar más ajustes en la configuración que el asistente (que sólo se ejecuta si va a configurar el servidor Web por primera vez). Incluye cuatro pestañas que se describen más adelante. Ningún cambio en las opciones de configuración que realice aquí surte efecto de forma

inmediata: debe confirmar los cambios con *Finalizar* para que se hagan efectivos. Si hace clic en *Cancelar,* se abandona el módulo de configuración y se descartan todos los cambios.

Puertos y direcciones de escucha

En *Servicio HTTP,* seleccione si Apache debe estar ejecutándose (*Activado*) o detenido (*Desactivado*). En *Escuchar en los puertos,* puede elegir entre *Añadir, Editar* o *Suprimir* direcciones y puertos en los que deba estar disponible el servidor. El ajuste predeterminado es que el servidor escuche en todas las interfaces del puerto 80. Debe seleccionar siempre *Abrir cortafuegos en los puertos seleccionados,* porque, si no lo hace, no se podrá acceder al servidor Web desde el exterior. Mantener el puerto de escucha cerrado es útil únicamente en situaciones de prueba en las que no es necesario el acceso externo al servidor Web.

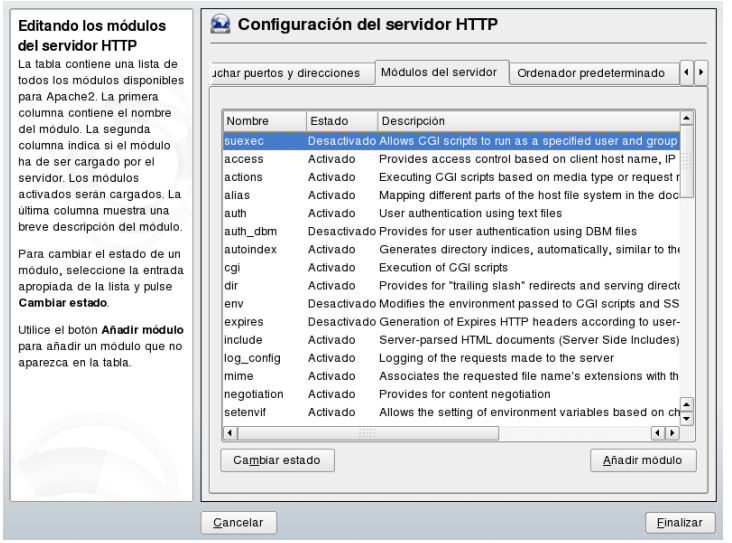
Mediante *Archivos de registro,* puede controlar el registro de acceso o el de errores, lo que resulta útil si quiere probar la configuración. El archivo de registro se abre en una ventana independiente desde la que puede también reiniciar o recargar el servidor Web (consulte la Sección 26.3, “Inicio y detención de Apache” (p. 500) para obtener información detallada). Estos comandos surten efecto de forma inmediata.

Figura 26.3 *Configuración del servidor HTTP: puertos y direcciones de escucha*

Módulos del servidor

Puede cambiar el estado (activado o desactivado) de los módulos de Apache2 haciendo clic en *Cambiar estado*. Haga clic en *Añadir módulo* para añadir un módulo nuevo que esté instalado pero que no aparezca en la lista. Para obtener más información acerca de los módulos, consulte la Sección 26.4, “Instalación, activación y configuración de módulos” (p. 502).

Figura 26.4 *Configuración del servidor HTTP: módulos del servidor*



Host o hosts por defecto

Estos cuadros de diálogo son idénticos a los que ya se han descrito. Consulte “Ordenador predeterminado” (p. 494) y “Hosts virtuales” (p. 497).

26.3 Inicio y detención de Apache

Si se configura con YaST (consulte la Sección 26.2.2, “Configuración de Apache con YaST” (p. 493)), Apache se inicia en el momento del arranque en los niveles de ejecución 3 y 5 y se detiene en los niveles de ejecución 0, 1, 2 y 6. Puede cambiar este comporta-

miento utilizando el editor de niveles de ejecución de YaST o la herramienta de la línea de comandos `chkconfig`.

Para iniciar, detener o manipular Apache en un sistema en ejecución, utilice el guión init `/usr/sbin/rcapache2` (consulte la Sección 8.2.2, “Guiones init” (p. 200) para obtener información general acerca de los guiones init). El comando `rcapache2` admite los siguientes parámetros:

`start`
: Inicia Apache en caso de que no se esté ejecutando todavía.

`startssl`
: Inicia Apache con compatibilidad para SSL en caso de que no se esté ejecutando todavía. Para obtener más información acerca de la compatibilidad para SSL, consulte la Sección 26.6, “Configuración de un servidor Web seguro con SSL” (p. 513).

`restart`
: Detiene y vuelve a iniciar Apache. Inicia el servidor Web en caso de que no se estuviera ejecutando antes.

`try-restart`
: Detiene y vuelve a iniciar Apache sólo si se estaba ejecutando antes.

`reload o graceful`
: Detiene el servidor Web advirtiendo a todos los procesos de Apache en horquilla que terminen primero sus peticiones antes de cerrar. A medida que se van finalizando los procesos, se van reemplazando por procesos iniciados nuevamente, lo que resulta en un “reinicio” completo de Apache.

SUGERENCIA

`rcapache2 reload` es el método más adecuado para reiniciar Apache en entornos de producción, por ejemplo, para activar un cambio en la configuración, ya que permite servir a todos los clientes sin causar cortes en la conexión.

`configtest`
: Comprueba la sintaxis de los archivos de configuración sin que afecte a un servidor Web en ejecución. Dado que esta comprobación se produce obligatoriamente cada

vez que el servidor se inicia, se vuelve a cargar o se reinicia, normalmente no es preciso ejecutarla explícitamente (si se detecta un error de configuración, el servidor Web no se inicia, no se vuelve a cargar o no se reinicia).

`probe`
: Evalúa la necesidad de volver a cargar el servidor (comprueba si la configuración ha cambiado) y sugiere los argumentos necesarios para el comando `rcapache2`.

`server-status y full-server-status`
: Muestra una pantalla de estado abreviada o completa, respectivamente. Requiere que estén instalados lynx o w3m, así como que esté activado el módulo mod_status. Además, se debe añadir `status` a `APACHE_SERVER_FLAGS` en el archivo `/etc/sysconfig/apache2`.

SUGERENCIA: Indicadores adicionales

Si especifica indicadores adicionales en `rcapache2`, éstos se transfieren a través del servidor Web.

26.4 Instalación, activación y configuración de módulos

El software de Apache está creado con un diseño modular: todas las funciones, excepto algunas tareas principales, están gestionadas por módulos. Este concepto se ha extendido hasta tal punto que incluso el protocolo HTTP se procesa mediante un módulo (http_core).

Los módulos de Apache pueden compilarse en el binario de Apache durante la generación, o cargarse de forma dinámica durante la ejecución. Consulte la Sección 26.4.2, “Activación y desactivación” (p. 503) para obtener información detallada acerca de cómo cargar los módulos de forma dinámica.

Los módulos de Apache se pueden dividir en cuatro categorías diferentes:

Módulos base
: Los módulos base están compilados en Apache por defecto. Apache en SUSE Linux cuenta sólo con mod_so (necesario para cargar otros módulos) y http_core compi-

lados. Todos los demás están disponibles como objetos compartidos: en lugar de estar incluidos en el binario del servidor en sí, se pueden incluir durante la ejecución.

Módulos de extensión
: Por regla general, los módulos etiquetados como "extensiones" se incluyen en el paquete de software de Apache, aunque normalmente no se compilan en el servidor de manera estática. En SUSE Linux, se encuentran disponibles como objetos compartidos que pueden cargarse en Apache en tiempo de ejecución.

Módulos externos
: Los módulos etiquetados como externos no se incluyen en la distribución oficial de Apache. Sin embargo, SUSE Linux ofrece algunos de ellos listos y disponibles para su uso.

Módulos de multiprocesamiento
: Los MPM son los responsables de aceptar y gestionar peticiones al servidor Web, por lo que representan el núcleo del software del servidor Web.

26.4.1 Instalación de módulos

Si ha seguido el método predeterminado durante la instalación de Apache (descrito en la Sección 26.1.2, “Instalación” (p. 484)), estará instalado con todos los módulos base y de extensión, con el módulo de multiprocesamiento MPM Prefork y el módulo externo PHP5.

Puede instalar otros módulos externos iniciando YaST y eligiendo *Software* → *Instalar/desinstalar software.* A continuación, elija *Filtro* → *Buscar* y busque *apache.* Entre otros paquetes, la lista de resultados incluirá todos los módulos externos de Apache disponibles.

26.4.2 Activación y desactivación

YaST permite activar o desactivar los módulos de lenguajes de guiones (PHP5, Perl, Python y Ruby) con la configuración de módulos que se describe en “Asistente de servidor HTTP” (p. 494). Los demás módulos se pueden activar o desactivar como se describe en “Módulos del servidor” (p. 500).

Si prefiere activar o desactivar los módulos manualmente, utilice los comandos `a2enmod` *`mod_foo`* o `a2dismod` *`mod_foo`*, respectivamente. `a2enmod -l` genera una lista de todos los módulos activos en cada momento.

IMPORTANTE: Inclusión de archivos de configuración para módulos externos

Si ha activado módulos externos manualmente, asegúrese de cargar los archivos de configuración correspondientes en todas las configuraciones de hosts virtuales. Los archivos de configuración de los módulos externos se ubican en `/etc/apache2/conf.d/` y no se cargan por defecto. Si necesita los mismos módulos en todos los hosts virtuales, puede incluir `*.conf` desde este directorio. Si no, deberá incluir los archivos individuales. Consulte `/etc/apache2/vhosts.d/vhost.template` para ver ejemplos.

26.4.3 Módulos base y de extensión

Todos los módulos base y de extensión se describen en profundidad en la documentación de Apache. Aquí se incluye únicamente una breve descripción de los módulos más importantes. Consulte `http://httpd.apache.org/docs/2.2/mod/` para conocer más detalles acerca de cada módulo.

mod_alias
: Proporciona las directivas `Alias` y `Redirect` (Redirigir) con las que puede asignar un URl a un directorio específico (`Alias`) o bien redirigir un URL solicitado a otra ubicación. Este módulo está habilitado por defecto.

mod_auth*
: Los módulos de autenticación proporcionan distintos métodos de autenticación: autenticación básica con mod_auth_basic o autenticación resumida con mod_auth_digest. Esta última se encuentra todavía en fase de experimentación en Apache 2.2.

  mod_auth_basic y mod_auth_digest se deben combinar con un módulo proveedor de autenticación, mod_authn_* (por ejemplo, mod_authn_file para la autenticación basada en archivo de texto) y con un módulo de autorización, mod_authz_* (por ejemplo, mod_authz_user para la autorización de usuarios).

Puede encontrar más información acerca de este tema en el tutorial sobre autenticación en la dirección http://httpd.apache.org/docs/2.2/howto/auth.html.

mod_autoindex
: Con autoindex se generan listas de directorios cuando no se cuenta con ningún archivo de índice (por ejemplo, `index.html`). El aspecto de los índices se puede configurar. Este módulo está habilitado por defecto. Sin embargo, las listas de directorios están deshabilitadas por defecto mediante la directiva `Options` (Opciones). Sobrescriba este ajuste en la configuración de host virtual. El archivo de configuración por defecto para este módulo se encuentra en `/etc/apache2/mod_autoindex-defaults.conf`.

mod_cgi
: mod_cgi es necesario para ejecutar guiones CGI. Este módulo está habilitado por defecto.

mod_deflate
: Con este módulo, se puede configurar Apache para que comprima determinados tipos de archivos directamente antes de entregarlos.

mod_dir
: mod_dir proporciona la directiva `DirectoryIndex` (Índice de directorios) con la que se puede configurar qué archivos se deben entregar automáticamente cuando se realiza una petición a un directorio (`index.html` por defecto). También proporciona una redirección automática al URI correcto cuando una petición de directorio no incluye una barra inclinada de cierre. Este módulo está habilitado por defecto.

mod_expires
: Con mod_expires, puede controlar la frecuencia con la que las memorias caché del alterno (proxy) y del navegador actualizan los documentos enviando un encabezado `Expires` (Caducidad). Este módulo está habilitado por defecto.

mod_include
: mod_include permite utilizar inclusiones de servidor (SSI, Server Side Includes), las cuales proporcionan la funcionalidad básica para generar páginas HTML de forma dinámica. Este módulo está habilitado por defecto.

mod_info
: Proporciona una descripción completa de la configuración del servidor en http://localhost/server-info/. Por razones de seguridad, debe limitar siempre el acceso a esta URL. Por defecto, sólo se puede acceder a esta URL desde `localhost`. mod_info se configura en `/etc/apache2/mod_info.conf`.

mod_log_config
: Con este módulo puede configurar el aspecto de los archivos de registro de Apache. Este módulo está habilitado por defecto.

mod_mime
: El módulo mime se encarga de que los archivos se entreguen con el encabezado MIME correcto basándose en la extensión del nombre de archivo (por ejemplo, `text/html` en el caso de documentos HTML). Este módulo está habilitado por defecto.

mod_negotiation
: Necesario para la negociación de contenido. Consulte `http://httpd.apache.org/docs/2.2/content-negotiation.html` para obtener más información. Este módulo está habilitado por defecto.

mod_rewrite
: Proporciona la funcionalidad de mod_alias, pero ofrece más funciones y mayor flexibilidad. Con mod_rewrite, puede redirigir URL a partir de distintas reglas, encabezados de petición, etc.

mod_speling
: mod_speling intenta corregir automáticamente errores tipográficos en las URL, como errores en el uso de mayúsculas.

mod_ssl
: Habilita las conexiones cifradas entre el servidor Web y los clientes. Para obtener más información, consulte la Sección 26.6, “Configuración de un servidor Web seguro con SSL” (p. 513). Este módulo está habilitado por defecto.

mod_status
: Proporciona información sobre la actividad y el rendimiento del servidor en http://localhost/server-status/. Por razones de seguridad, debe limitar siempre el acceso a esta URL. Por defecto, sólo se puede acceder a esta URL desde `localhost`. mod_status se configura en `/etc/apache2/mod_status.conf`

mod_suexec
: mod_suexec permite ejecutar guiones CGI con un usuario y un grupo distintos. Este módulo está habilitado por defecto.

mod_userdir
: Habilita directorios específicos de usuario disponibles en `~usuario/`. La directiva `UserDir` (Directorio de usuario) se debe especificar en la configuración. Este módulo está habilitado por defecto.

26.4.4 Módulos de multiprocesamiento

SUSE Linux ofrece dos módulos de multiprocesamiento (MPM) distintos para su uso con Apache.

Módulo MPM prefork

El módulo MPM prefork implementa un servidor Web sin hilos y previo a la bifurcación. Hace que el servidor Web se comporte de manera similar a la versión 1.x de Apache en el sentido en que aísla cada petición y la gestiona bifurcando un proceso hijo independiente. Por lo tanto, las peticiones problemáticas no pueden afectar a otras, lo que evita el bloqueo del servidor Web.

A pesar de que ofrece más estabilidad gracias a este enfoque basado en procesos, el módulo MPM prefork consume más recursos de sistema que su homólogo, el módulo MPM worker. El módulo MPM prefork está considerado el MPM por defecto para los sistemas operativos basados en Unix.

IMPORTANTE: MPM en este documento

En este documento se presupone que se utiliza Apache con el módulo MPM prefork.

Módulo MPM worker

El módulo MPM worker ofrece un servidor Web de múltiples hilos. Un hilo es una forma “más ligera” de un proceso. La ventaja de un hilo sobre un proceso es el bajo consumo de recursos. En lugar de bifurcar sólo procesos hijo, el módulo MPM worker responde a las peticiones mediante hilos con los procesos del servidor. Los procesos

hijos previos a la bifurcación son de múltiples hilos. Este enfoque mejora el rendimiento de Apache al consumir menos recursos de sistema que el módulo MPM prefork.

Un gran inconveniente es la estabilidad del módulo MPM worker: si un hilo se daña, todos los hilos de un proceso pueden verse afectados. En el peor de los casos, puede llevar a que el servidor se bloquee. Sobre todo cuando se usa CGI (Common Gateway Interface, interfaz de gateway común) con Apache y hay una carga intensa, se pueden producir errores internos de servidor debidos a hilos que no pueden comunicarse con los recursos del sistema. Otro argumento en contra del uso de MPM worker con Apache es que no todos los módulos de Apache disponibles son hilos de proceso seguro y, por lo tanto, no pueden usarse con MPM worker.

AVISO: Utilización de módulos PHP con MPM

No todos los módulos PHP disponibles son hilos de proceso seguro. Se desaconseja encarecidamente el uso de MPM worker con mod_php.

26.4.5 Módulos externos

Aquí se recoge una lista de todos los módulos externos que se incluyen con SUSE Linux. La documentación de cada módulo se encuentra en el directorio señalado.

FastCGI
: FastCGI es una extensión independiente de lenguaje, ampliable y abierta para CGI que proporciona un alto rendimiento sin las limitaciones de las API específicas de servidores. Las aplicaciones FastCGI ofrecen una gran velocidad porque son permanentes: no se inician por petición ni se da sobrecarga en el inicio.

  Nombre del paquete: `apache2-mod_fastcgi`
  Archivo de configuración: `/etc/apache2/conf.d/mod_fastcgi.conf`
  Más información: `/usr/share/doc/packages/apache2-mod_fastcgi`

mod_perl
: mod_perl permite ejecutar guiones Perl en un intérprete integrado. El intérprete permanente integrado en el servidor evita la sobrecarga debido al inicio de un intérprete externo y la ralentización debida al tiempo de inicio de Perl.

  Nombre del paquete: `apache2-mod_perl`
  Archivo de configuración: `/etc/apache2/conf.d/mod_perl.conf`

Más información: `/usr/share/doc/packages/apache2-mod_perl`

mod_php5
: PHP es un lenguaje de guiones de servidor HTML multiplataforma integrado.

  Nombre del paquete: `apache2-mod_php5`
  Archivo de configuración: `/etc/apache2/conf.d/php5.conf`
  Más información: `/usr/share/doc/packages/apache2-mod_php5`

mod_python
: mod_python permite la incrustación de Python en el servidor HTTP Apache para obtener un rendimiento mucho mayor y flexibilidad adicional para el diseño de aplicaciones basadas en Web.

  Nombre del paquete: `apache2-mod_python`
  Más información: `/usr/share/doc/packages/apache2-mod_python`

mod_ruby
: mod_ruby incrusta el intérprete Ruby en el servidor Web Apache, lo que permite que los guiones CGI de Ruby se ejecuten de forma interna. Los guiones se inician mucho más rápido que sin mod_ruby.

  Nombre del paquete: `apache2-mod_ruby`
  Más información: `/usr/share/doc/packages/apache2-mod_ruby`

mod_jk-ap20
: Este módulo proporciona conectores entre Apache y un contenedor servlet Tomcat.

  Nombre del paquete: `mod_jk-ap20`
  Más información: `/usr/share/doc/packages/mod_jk-ap20`

26.4.6 Compilación

Los usuarios avanzados pueden ampliar Apache creando módulos personalizados. Para desarrollar módulos de Apache o compilar módulos de otros fabricantes, es necesario disponer del paquete `apache2-devel`, junto con las correspondientes herramientas de desarrollo. `apache2-devel` contiene también las herramientas `apxs2`, necesarias para compilar módulos adicionales para Apache.

`apxs2` habilita la compilación e instalación de módulos a partir del código fuente (incluidos los cambios necesarios en los archivos de configuración), tras lo cual se crean *objetos compartidos dinámicos* (DSO) que se pueden cargar en Apache en tiempo de ejecución.

Los binarios `apxs2` se encuentran en `/usr/sbin`:

- `/usr/sbin/apxs2`: adecuado para crear un módulo de extensión que funcione con cualquier MPM. La ubicación de instalación es `/usr/lib/apache2`.
- `/usr/sbin/apxs2-prefork`: adecuado para módulos MPM de prefork. La ubicación de instalación es `/usr/lib/apache2-prefork`.
- `/usr/sbin/apxs2-worker`: adecuado para módulos MPM de worker.

`apxs2` instala módulos que todos los MPM puedan utilizar. Los otros dos programas instalan módulos que sólo pueden utilizar los MPM respectivos. `apxs2` instala módulos en `/usr/lib/apache2`, y `apxs2-prefork` y `apxs2-worker` instalan módulos en `/usr/lib/apache2-prefork` o `/usr/lib/apache2-worker`.

Puede instalar y activar un módulo a partir de código fuente con los comandos `cd /path/to/module/source; apxs2 -cia` *`mod_foo`*`.c` (`-c` compila el módulo, `-i` lo instala y `-a` lo activa). Las otras opciones de `apxs2` se describen en la página Man `apxs2(1)`.

26.5 Puesta en funcionamiento de guiones CGI

La interfaz de gateway común (CGI) de Apache permite crear contenido dinámico con programas o guiones que normalmente se conocen como guiones CGI. En teoría, se pueden escribir guiones CGI en cualquier lenguaje de programación. Por lo general se emplean lenguajes de guiones como Perl o PHP.

Para hacer que Apache proporcione contenido creado mediante guiones CGI, se debe activar mod_cgi. También es necesario mod_alias. Ambos módulos están habilitados por defecto. Consulte la Sección 26.4.2, “Activación y desactivación” (p. 503) para obtener información detallada acerca de la activación de módulos.

AVISO: Seguridad de CGI

Cuando se permite que el servidor ejecute guiones CGI se genera una brecha potencial en la seguridad. Consulte la Sección 26.7, “Cómo evitar problemas de seguridad” (p. 520) para obtener más información.

26.5.1 Configuración de Apache

En SUSE Linux, la ejecución de guiones CGI sólo está permitida en el directorio `/srv/www/cgi-bin/`. Esta ubicación está configurada de antemano para ejecutar guiones CGI. Si ha creado una configuración de host virtual (consulte “Configuración de hosts virtuales” (p. 489)) y quiere colocar los guiones en un directorio específico de hosts, debe desbloquear y configurar ese directorio.

Ejemplo 26.5 *Configuración de CGI para VirtualHost*

```
ScriptAlias /cgi-bin/ "/srv/www/example.com_cgi-bin/"❶

<Directory "/srv/www/example.com_cgi-bin/">
 Options +ExecCGI❷
 AddHandler cgi-script .cgi .pl❸
 Order allow,deny❹
 Allow from all
</Directory>
```

❶ Indica a Apache que debe tratar todos los archivos de este directorio como guiones CGI.

❷ Habilita la ejecución de guiones CGI.

❸ Indica al servidor que debe tratar los archivos con las extensiones .pl y .cgi como guiones CGI. Se puede ajustar según las distintas necesidades.

❹ Las directivas `Order` (Orden) y `Allow` (Permitir) controlan el estado de acceso por defecto y el orden en el que se evalúan las directivas Allow (Permitir) y Deny (Denegar). En este caso, las sentencias “deny” (denegar) se evalúan antes que las sentencias “allow” (permitir) y se habilita el acceso desde cualquier parte.

26.5.2 Ejecución de un guión de ejemplo

La programación de CGI se diferencia de la programación "normal" en que los programas y guiones CGI deben ir precedidos de un encabezado de tipo MIME, como `Content-type: text/html`. Este encabezado se envía al cliente para que entienda el tipo de contenido que recibe. En segundo lugar, la salida de los guiones debe ser algo que el cliente, normalmente un navegador Web, entienda: como HTML en la mayoría de los casos, texto sin formato o imágenes, por ejemplo.

El paquete de Apache incluye un guión simple de prueba en `/usr/share/doc/packages/apache2/test-cgi`. Con él se genera el contenido de algunas variables de entorno como texto sin formato. Copie este guión en `/srv/www/cgi-bin/` o en el directorio de guiones de su host virtual (/srv/www/example.com_cgi-bin/) y asígnele el nombre `test.cgi`.

Los archivos a los que pueda acceder el servidor Web deben ser propiedad del usuario `Root` (consulte la Sección 26.7, “Cómo evitar problemas de seguridad” (p. 520) para obtener más información). Dado que el servidor Web se ejecuta con un usuario distinto, los guiones CGI deben poder ejecutarse y leerse globalmente. Acceda al directorio de CGI y utilice el comando `chmod 755 test.cgi` para aplicar los permisos adecuados.

A continuación, llame a `http://localhost/cgi-bin/test.cgi` o `http://example.com/cgi-bin/test.cgi`. Debería aparece el informe de prueba de guión “CGI/1.0 test script report”.

26.5.3 Solución de problemas

Si no se muestra el resultado del programa de prueba, sino un mensaje de error, compruebe lo siguiente:

Solución de problemas de CGI

- ¿Ha vuelto a cargar el servidor después de cambiar la configuración? Compruébelo con `rcapache2 probe`.
- Si ha configurado un directorio de CGI personalizado, ¿está configurado correctamente? Si no está seguro, pruebe el guión dentro del directorio CGI por defecto,

`/srv/www/cgi-bin/`, y actívelo con `http://localhost/cgi-bin/test.cgi`.

- ¿Son correctos los permisos de archivo? Acceda al directorio de CGI y ejecute el comando `ls -l test.cgi`. El resultado debe comenzar con

  ```
  -rwxr-xr-x  1 root root
  ```

- Asegúrese de que el guión no incluya errores de programación. No debería ocurrir si no ha cambiado el archivo test.cgi; pero, si utiliza programas propios, asegúrese siempre de que no contengan errores de programación.

26.6 Configuración de un servidor Web seguro con SSL

Siempre que se deban transferir datos confidenciales, como información de tarjetas de crédito, entre el servidor Web y el cliente, es aconsejable contar con una conexión segura y cifrada que incluya autenticación. mod_ssl proporciona un potente cifrado mediante los protocolos de nivel de zócalo con seguridad (SSL) y de seguridad del nivel de transporte (TLS) para la comunicación HTTP entre un cliente y un servidor Web. Mediante SSL/TSL se establece una conexión privada entre el servidor Web y el cliente. Se asegura la integridad de los datos y el cliente y el servidor pueden autenticarse mutuamente.

Para este propósito, el servidor envía un certificado SSL con información que prueba la identidad válida del servidor antes de responder a cualquier petición a una URL. A su vez, de esta manera se garantiza que el servidor es el único punto final correcto de la comunicación. Además, el certificado genera una conexión cifrada entre el cliente y el servidor que puede transportar información sin el riesgo de exponer contenido importante en formato de sólo texto.

mod_ssl no implementa los protocolos SSL/TSL por sí mismo, sino que actúa como interfaz entre Apache y una biblioteca SSL. En SUSE Linux, se emplea la biblioteca OpenSSL, la cual se instala automáticamente con Apache.

El efecto más visible de usar mod_ssl con Apache es que las URL van precedidas de `https://` en lugar de `http://`.

26.6.1 Creación de un certificado SSL

Para utilizar SSL/TSL con el servidor Web, debe crear un certificado SSL. Este certificado es necesario para la autorización entre el servidor Web y el cliente de modo que cada parte pueda identificar claramente a la otra parte. Para garantizar la integridad del certificado, debe estar firmado por una parte en la que confíen todos los usuarios.

Se pueden crear tres tipos de certificados distintos: un certificado "ficticio" con fines de prueba únicamente, un certificado autofirmado para un grupo de usuarios determinado que confíen en usted o un certificado firmado por una autoridad certificadora (CA) independiente y conocida públicamente.

La creación de un certificado es un proceso en dos pasos básicamente. En primer lugar, se genera una clave privada para la autoridad certificadora y después el certificado del servidor se firma con esta clave.

SUGERENCIA: Información adicional

Para obtener más información acerca de los conceptos y definiciones de SSL/TSL, consulte `http://httpd.apache.org/docs/2.2/ssl/ssl_intro.html`.

Creación de un certificado "ficticio"

La creación de un certificado ficticio es fácil. Basta con llamar al guión `/usr/bin/gensslcert`. De esta forma se crean o sobrescriben los archivos siguientes:

- `/etc/apache2/ssl.crt/ca.crt`
- `/etc/apache2/ssl.crt/server.crt`
- `/etc/apache2/ssl.key/server.key`
- `/etc/apache2/ssl.csr/server.csr`

También se coloca una copia de `ca.crt` en `/srv/www/htdocs/CA.crt` para su descarga.

IMPORTANTE

los certificados ficticios no se deben emplear nunca en un sistema de producción. Sólo se deben utilizar con fines de prueba.

Creación de un certificado autofirmado

Si está configurando un servidor Web seguro para una intranet o un grupo de usuarios definido, puede que sea suficiente firmar un certificado con su propia autoridad certificadora (CA).

La creación de un certificado autofirmado constituye un proceso interactivo en nueve pasos. Acceda al directorio `/usr/share/doc/packages/apache2` y ejecute el siguiente comando: `./mkcert.sh make --no-print-directory /usr/bin/openssl /usr/sbin/ custom`. No intente ejecutar este comando desde otra ubicación que no sea ese directorio. El programa proporciona una serie de solicitudes, algunas de las cuales requieren que el usuario proporcione información.

Procedimiento 26.1 *Creación de un certificado autofirmado con mkcert.sh*

1 `Decida el algoritmo de firma que se deba utilizar para los certificados.`

Elija RSA (R , valor por defecto), puesto que algunos navegadores antiguos presentan problemas con DSA.

2 `Generación de una clave privada RSA para CA (1024 bits)`

No se requiere ninguna interacción.

3 `Generación de una petición de firma de certificado X.509 para CA`

Cree aquí el nombre completo de la CA. Este paso requiere que conteste a algunas preguntas, como el país o el nombre de la organización. Escriba datos válidos, puesto que todo lo que escriba aquí se mostrará después en el certificado. No es preciso que conteste a todas las preguntas. Si alguna no se aplica a su caso o quiere dejarla en blanco, utilice "." (un punto). El nombre común es el nombre de la CA en sí: elija un nombre con sentido, como *`CA de mi empresa`*.

4 `Generación de un certificado X.509 para la CA firmado por ella misma`

Elija la versión de certificado [3] (valor por defecto).

5 `Generación de una clave privada RSA para el servidor (1024 bits)`

No se requiere ninguna interacción.

6 `Generación de una petición de firma de certificado X.509 para el servidor`

Cree el nombre completo para la clave del servidor aquí. Las preguntas son prácticamente idénticas a las que ya ha respondido en relación con el nombre completo de la CA. La información que se proporciona aquí se aplica al servidor Web y no tiene necesariamente que ser idéntica a los datos correspondientes a la CA (por ejemplo, puede ser que el servidor esté ubicado en otro lugar).

IMPORTANTE: Selección de un nombre común

El nombre común que escriba aquí debe ser el nombre de host completo o del servidor seguro (por ejemplo, www.ejemplo.com). Si no, el navegador advertirá de que el certificado no coincide con el servidor cuando acceda al servidor Web.

---

7 `Generación de un certificado X.509 firmado por la CA propia`

Elija la versión de certificado [3] (valor por defecto).

8 `Cifrado de la clave privada RSA de la CA con una contraseña codificada por razones de seguridad`

Se recomienda encarecidamente cifrar la clave privada de la CA con una contraseña, por lo que debe elegir [Y] e introducir una contraseña.

9 `Cifrado de la clave privada RSA del servidor con una contraseña codificada por razones de seguridad`

El cifrado de la clave del servidor con una contraseña requiere que se escriba la contraseña cada vez que se inicie el servidor Web. Con esto se dificulta el inicio automático del servidor durante el arranque o el reinicio del servidor Web. Por lo tanto, el sentido común aconseja responder [N] a esta pregunta. Tenga en cuenta que la clave se queda sin proteger cuando no se cifra con una contraseña y asegúrese de que sólo personas autorizadas tengan acceso a esa clave.

IMPORTANTE: Cifrado de la clave del servidor

Si decide cifrar la clave del servidor con una contraseña, aumente el valor de APACHE_TIMEOUT en `/etc/sysconfig/apache2`. Si no lo hace, no tendrá tiempo suficiente para escribir la contraseña codificada antes de que el intento de inicio del servidor se pare y no tenga éxito.

La página de resultados del guión presenta una lista de los certificados y las claves que ha generado. En contra de lo que se muestra en el resultado del guión, los archivos no se generan en el directorio `conf` local, sino en las ubicaciones correctas dentro de `/etc/apache2/`.

El último paso consiste en copiar el archivo de certificado de CA de `/etc/apache2/ssl.crt/ca.crt` a una ubicación donde los usuarios puedan acceder a él con el fin de incorporarlo en la lista de CA conocidas y de confianza de sus navegadores Web. Si no se hace así, el navegador indicará que el certificado ha sido emitido por una autoridad desconocida. El certificado es válido durante un año.

IMPORTANTE: certificados autofirmados

Sólo se deben utilizar certificados autofirmados en servidores Web a los que accedan personas que le conozcan y confíen en usted en calidad de autoridad certificadora. No se recomienda utilizar ese tipo de certificados en una tienda pública, por ejemplo.

Obtención de certificados firmados oficialmente

Existen diversas autoridades certificadoras oficiales que pueden firmar sus certificados. El certificado lo firma una parte digna de confianza, por lo que se puede confiar en él totalmente. Los servidores Web seguros públicos normalmente disponen de un certificado firmado oficialmente.

Las CA oficiales más conocidas son Thawte (`http://www.thawte.com/`) y Verisign (`www.verisign.com`). Éstas y otras CA ya están compiladas en todos los navegadores, por lo que los certificados firmados por estas autoridades se aceptan automáticamente en ellos.

Cuando se solicita un certificado firmado oficialmente, no se envía un certificado a la CA, sino que se emite una petición de firma de certificado (CSR, Certificate Signing Request). Para crear una CSR, se debe llamar al guión `/usr/share/ssl/misc/CA.sh -newreq`.

En primer lugar, el guión solicita una contraseña con la que se debe cifrar la CSR. Después, se le pide que escriba un nombre completo. Este paso requiere que conteste a algunas preguntas, como el país o el nombre de la organización. Escriba datos válidos: todo lo que escriba aquí se mostrará más adelante en el certificado y se comprobará. No es preciso que conteste a todas las preguntas. Si alguna no se aplica a su caso o quiere dejarla en blanco, utilice "." (un punto). El nombre común es el nombre de la CA en sí: elija un nombre con sentido, como *`CA de mi empresa`*. Por último, se deben proporcionar una contraseña de verificación y un nombre de empresa alternativo.

La CSR se genera en el directorio desde el que se llama al guión y el archivo recibe el nombre `newreq.pem`.

26.6.2 Configuración de Apache con SSL

El puerto por defecto para las peticiones de SSL y TLS en el servidor Web es el 443. No hay conflicto entre una escucha "normal" de Apache en el puerto 80 y una escucha de Apache habilitada para SSL/TLS en el puerto 443. De hecho, HTTP y HTTPS pueden ejecutarse con la misma instancia de Apache. Normalmente se emplean hosts virtuales independientes para expedir peticiones al puerto 80 y al puerto 443 para servidores virtuales independientes.

IMPORTANTE: Configuración del cortafuegos

No olvide abrir el puerto 443 en el cortafuegos para Apache habilitado para SSL, lo que se puede hacer mediante YaST, como se describe en "Configuración con YaST" (p. 116).

Para utilizar SSL, se debe activar en la configuración de servidor global. Abra `/etc/sysconfig/apache2` en un editor y busque `APACHE_MODULES`. Añada "ssl" a

la lista de módulos si no está incluido todavía (mod_ssl se activa por defecto). A continuación, busque APACHE_SERVER_FLAGS y añada "SSL". Si ha decidido cifrar el certificado de servidor con una contraseña, debe también aumentar el valor de APACHE_TIMEOUT con el fin de disponer del tiempo suficiente para escribir la contraseña codificada cuando se inicie Apache. Reinicie el servidor para que los cambios se activen. No basta con volver a cargarlo.

El directorio de configuración de host virtual incluye una plantilla, `/etc/apache2/vhosts.d/vhost-ssl.template`, con directivas específicas para SSL ampliamente documentadas. Consulte "Configuración de hosts virtuales" (p. 489) para conocer la configuración general del host virtual.

Para comenzar, debería bastar con ajustar los valores de las directivas siguientes:

- `DocumentRoot`
- `ServerName`
- `ServerAdmin`
- `ErrorLog`
- `TransferLog`

IMPORTANTE: Hosts y SSL virtuales basados en nombres

No es posible ejecutar varios hosts virtuales habilitados para SSL en un servidor con una única dirección IP. Los usuarios que se conectan a una configuración de este tipo reciben un mensaje de advertencia en el que se les indica que el certificado no coincide con el nombre del servidor cada vez que visitan una URL. Se necesita una dirección IP o puerto distintos para cada dominio habilitado para SSL para poder comunicarse basándose en un certificado SSL válido.

26.7 Cómo evitar problemas de seguridad

Un servidor Web expuesto al público en Internet requiere un esfuerzo de administración constante. Es inevitable que aparezcan problemas de seguridad, relacionados tanto con el software como con errores de configuración accidentales. A continuación se ofrecen algunos consejos sobre cómo actuar al respecto.

26.7.1 Software actualizado

Cuando se detecten vulnerabilidades en el software Apache, SUSE emitirá un comunicado de seguridad. En él se incluirán instrucciones para reparar las vulnerabilidades, que deberán aplicarse lo antes posible. Los avisos de seguridad de SUSE están disponibles en las siguientes ubicaciones:

- **Página Web** `http://www.suse.com/us/private/support/online_help/mailinglists/`
- **Lista de correo** `http://www.suse.com/us/private/support/online_help/mailinglists/`
- **Suministro RSS** `http://www.novell.com/linux/security/suse_security.xml`

26.7.2 Permisos de DocumentRoot

En SUSE Linux, los directorios `DocumentRoot` (`/srv/www/htdocs`) y CGI (`/srv/www/cgi-bin`) pertenecen por defecto al usuario y al grupo `root`. No debe modificar estos permisos. Si estos directorios conceden permiso de escritura a cualquier usuario, cualquiera podría colocar archivos en ellos. Si se diera el caso, esos archivos podrían ejecutarse en Apache con los permisos de `wwwrun`, lo que podría proporcionar acceso a los recursos del sistema de archivos a usuarios que no deberían tenerlo. Utilice subdirectorios `/srv/www` para colocar los directorios `DocumentRoot` y CGI para los hosts virtuales y asegúrese de que los directorios y los archivos pertenezcan al usuario y al grupo `Root`.

26.7.3 Acceso al sistema de archivos

Por defecto, el acceso a todo el sistema de archivos se deniega mediante `/etc/apache2/httpd.conf`. No debe sobrescribir estas directivas en ningún momento, sino habilitar específicamente el acceso a todos los directorios que Apache debe poder leer (consulte "Configuración básica de host virtual" (p. 492) para obtener información detallada). Cuando lo haga, asegúrese de que no se puedan leer desde el exterior archivos importantes, como archivos de contraseñas o de configuración del sistema.

26.7.4 Guiones CGI

Los guiones interactivos de Perl, PHP, SSI o cualquier otro lenguaje de programación pueden ejecutar comandos arbitrarios, por lo que presentan un problema general para la seguridad. Los guiones que se deban ejecutar desde el servidor sólo se deben instalar a partir de fuentes en las que confíe el administrador del servidor. Por lo general no es aconsejable permitir que los usuarios ejecuten sus propios guiones. También se recomienda realizar auditorías de seguridad de todos los guiones.

Para que la administración de los guiones resulte lo más fácil posible, se suele limitar la ejecución de guiones CGI a directorios específicos, en lugar de permitirlos de forma global. Las directivas `ScriptAlias` (Alias de guión) y `Option ExecCGI` (Opción ExecCGI) se utilizan en la configuración. Con la configuración por defecto de SUSE Linux no se permite la ejecución de guiones CGI desde cualquier lugar.

Todos los guiones CGI se ejecutan desde el mismo usuario, por lo que los distintos guiones pueden entrar en conflicto entre sí. El módulo suEXEC permite ejecutar guiones CGI con un usuario y un grupo distintos.

26.7.5 Directorios de usuario

Cuando habilite directorios de usuario (con mod_userdir o mod_rewrite), debería considerar seriamente no permitir archivos `.htaccess`, los cuales dan a los usuarios la capacidad de sobrescribir ajustes de seguridad. Al menos debería limitar las posibilidades de los usuarios mediante la directiva `AllowOverRide` (Permitir sobrescritura). En SUSE Linux, los archivos `.htaccess` están habilitados por defecto, pero los usuarios no tienen permiso para sobrescribir ninguna directiva `Option` (Opción) al

utilizar mod_userdir (consulte el archivo de configuración `/etc/apache2/mod_userdir.conf`).

26.8 Solución de problemas

Si Apache no se inicia, no se puede acceder a la página Web o los usuarios no pueden conectarse al servidor Web, es importante descubrir el motivo del problema. A continuación describiremos algunos lugares habituales en los que se debe buscar las explicaciones de los errores y algunos aspectos importantes que se deben comprobar.

En primer lugar, `rcapache2` (descrito en la Sección 26.3, “Inicio y detención de Apache” (p. 500)) proporciona un informe detallado sobre los errores, de modo que puede resultar bastante útil si se utiliza para controlar Apache. Algunas veces puede resultar tentador emplear el binario `/usr/sbin/httpd2` para iniciar o detener el servidor Web. Evite hacerlo y emplee el guión `rcapache2` en su lugar. `rcapache2` proporciona incluso sugerencias y consejos para resolver errores de configuración.

En segundo lugar, nunca se debe subestimar la importancia de los archivos de registro. Los archivos de registro de Apache, principalmente el archivo de registro de errores, permiten buscar las causas de errores fatales y de cualquier otro tipo. Además, se puede controlar el nivel de detalle de los mensajes registrados con la directiva `LogLevel` (Nivel de registro) si se necesita un nivel mayor de detalle en los archivos de registro. El archivo de registro de errores está ubicado por defecto en `/var/log/apache2/error_log`.

SUGERENCIA: una sencilla prueba

Observe los mensajes de registro de Apache con el comando `tail -F /var/log/apache2/`*`mi_registro_de_errores`*. A continuación, ejecute `rcapache2 restart`. Ahora intente conectarse con un navegador y compruebe los resultados.

Un error muy común es el de no abrir los puertos para Apache en la configuración del cortafuegos del servidor. Si ha configurado Apache con YaST, hay una opción independiente disponible para encargarse de este problema específico (consulte la Sección 26.2.2, “Configuración de Apache con YaST” (p. 493)). Si está configurando Apache manualmente, abra los puertos del cortafuegos para HTTP y HTTPS a través del módulo de cortafuegos de YaST.

Si no puede realizarse un seguimiento del error con la ayuda de ninguno de estos medios, compruebe la base de datos de errores en línea de Apache en http://httpd.apache.org/bug_report.html. También existe la posibilidad de comunicarse con la comunidad de usuarios de Apache a través de una lista de correo, disponible en http://httpd.apache.org/userslist.html. Por último, desde comp.infosystems.www.servers.unix accederá a un grupo de noticias muy recomendable.

26.9 Información adicional

El paquete apache2-doc incluye el manual de Apache completo en varios idiomas para la instalación local y como referencia. No se instala por defecto. El modo más rápido para instalarlo es mediante el comando yast -i apache2-doc. Una vez instalado, el manual de Apache se encuentra en http://localhost/manual/. También puede encontrarlo en Web, en la dirección http://httpd.apache.org/docs-2.2/. Puede obtener consejos de configuración específicos de SUSE en el directorio /usr/share/doc/packages/apache/README.*.

26.9.1 Apache 2.2

Si desea conocer las nuevas funciones de Apache 2.2, consulte http://httpd.apache.org/docs/2.2/new_features_2_2.html. En http://httpd.apache.org/docs-2.2/upgrading.html podrá consultar información acerca de cómo actualizar la versión 2.0 a la 2.2.

26.9.2 Módulos de Apache

Podrá consultar más información acerca de los módulos de Apache externos de la Sección 26.4.5, “Módulos externos” (p. 508) en las siguientes direcciones:

FastCGI
http://www.fastcgi.com/

mod_perl
http://perl.apache.org/

mod_php5
http://www.php.net/manual/en/install.unix.apache2.php

mod_python
http://www.modpython.org/

mod_ruby
http://www.modruby.net/

26.9.3 Desarrollo

Puede obtener información adicional acerca del desarrollo de módulos de Apache o de cómo involucrarse en el proyecto del servidor Web Apache en las siguientes ubicaciones:

Información para desarrolladores de Apache
http://httpd.apache.org/dev/

Documentación para desarrolladores de Apache
http://httpd.apache.org/docs/2.2/developer/

Escritura de módulos de Apache con Perl y C
http://www.modperl.com/

26.9.4 Fuentes varias

Si experimenta dificultades relacionadas específicamente con Apache en SUSE Linux, consulte la base de datos de asistencia de SUSE en http://portal.suse.com/sdb/en/index.html. En http://httpd.apache.org/ABOUT_APACHE.html podrá leer información acerca del origen y la evolución de Apache. Esta página explica también por qué el servidor se llama Apache.

27 Sincronización de archivos

Hoy en día, muchas personas utilizan varios equipos: uno en casa, otro o varios en el trabajo y un portátil o PDA cuando están de viaje. Se necesitan muchos archivos en todos estos equipos. Resulta conveniente poder trabajar con ellos y que, al modificar los archivos, las versiones más recientes de los datos estén disponibles en todos los equipos.

27.1 Software de sincronización de datos disponible

La sincronización de datos no supone un problema para los equipos que están enlazados de forma permanente a través de una red rápida. En estos casos, la utilización de un sistema de archivos de red, como NFS, y el almacenamiento de los archivos en un servidor hacen posible que todos los hosts accedan a los mismos datos mediante la red. Este enfoque no es factible si la conexión de red es de escasa calidad o no es permanente. Si está de viaje con un portátil, necesitará disponer de copias de los archivos necesarios en el disco duro local. Sin embargo, en ese caso es necesario sincronizar los archivos modificados. Al modificar un archivo en un equipo, asegúrese de que se actualiza una copia del archivo en todos los demás equipos. En el caso de copias ocasionales, esta tarea puede llevarse a cabo manualmente mediante scp o rsync. No obstante, si hay muchos archivos implicados, el procedimiento puede resultar complicado y requerir mucho cuidado para evitar errores, como la sobrescritura de un archivo más reciente por uno anterior.

AVISO: Riesgo de pérdida de datos

Antes de empezar a gestionar los datos con un sistema de sincronización, debe estar bien familiarizado con el programa que vaya a emplear y comprobar sus funciones. Resulta indispensable disponer de una copia de seguridad de los archivos importantes.

La tarea de sincronización manual, que requiere mucho tiempo y propicia que se produzcan errores, puede evitarse empleando uno de los programas que utilizan distintos métodos para automatizar este trabajo. Los siguientes resúmenes sólo pretenden ofrecer una descripción general del funcionamiento de estos programas y el modo en que pueden utilizarse. Si tiene previsto utilizarlos, lea la documentación de los programas.

27.1.1 Unison

Unison no es un sistema de archivos de red. En su lugar, los archivos sencillamente se guardan y editan en una ubicación local. El programa Unison puede ejecutarse manualmente para sincronizar archivos. Cuando la sincronización se lleva a cabo por primera vez, se crea una base de datos en ambos hosts que contiene las sumas de control, las marcas horarias y los permisos de los archivos seleccionados. En la siguiente ejecución, Unison reconoce los archivos modificados y propone la transmisión desde un host o el otro. Normalmente se pueden aceptar todas las sugerencias.

27.1.2 CVS

CVS, que normalmente se utiliza para gestionar versiones de programas, ofrece la posibilidad de conservar copias de los archivos en varios equipos. Por lo tanto, también es adecuado para la sincronización de datos. CVS mantiene un repositorio central en el servidor, donde se almacenan los archivos y los cambios realizados en ellos. Los cambios realizados localmente se asignan al repositorio y se pueden recuperar desde otros equipos mediante actualizaciones. El usuario debe iniciar manualmente ambos procedimientos.

CVS es muy resistente a los errores cuando los cambios se producen en varios equipos. Los cambios se fusionan y, si se producen cambios distintos en las mismas líneas, se informa acerca del conflicto. Cuando se produce un conflicto, la base de datos sigue

conservando la coherencia. El conflicto sólo aparece en el host del cliente, a fin de que sea posible resolverlo.

27.1.3 Subversion

En contraste con CVS, que "evolucionó" de forma espontánea, Subversion (SVN) es un proyecto diseñado de forma coherente. Subversion se desarrolló como un sucesor de CVS mejorado técnicamente.

Subversion supera en muchos aspectos a su predecesor. Debido a su historia de desarrollo, CVS sólo conserva archivos y obvia los directorios. En Subversion, los directorios también tienen un historial de versiones y existe la posibilidad de copiarlos y modificar sus nombres, del mismo modo que ocurre con los archivos. También es posible añadir metadatos a todos los archivos y directorios. Estos metadatos pueden mantenerse totalmente en las sucesivas versiones. A diferencia de CVS, Subversion es compatible con el acceso transparente a la red mediante protocolos dedicados, como WebDAV (del inglés Web-based Distributed Authoring and Versioning, versiones y autoría distribuidas basadas en Web). WebDAV amplía la funcionalidad del protocolo HTTP para permitir acceso de escritura de colaboración en los archivos de servidores Web remotos.

Subversion se generó en gran medida a partir de paquetes de software existentes. Por lo tanto, el servidor Web Apache y la extensión WebDAV siempre deben ejecutarse con Subversion.

27.1.4 mailsync

A diferencia de las herramientas de sincronización descritas en las secciones anteriores, mailsync sólo sincroniza mensajes de correo electrónico entre buzones. El procedimiento puede aplicarse a archivos de buzón locales y a buzones de un servidor IMAP.

En función del identificador de mensaje que incluya el encabezado, los mensajes individuales se sincronizan o se suprimen. Existe la posibilidad de llevar a cabo la sincronización entre buzones individuales y entre jerarquías de buzones.

27.1.5 rsync

Cuando no es necesario controlar las versiones, pero sí sincronizar grandes estructuras de directorios en conexiones de red lentas, la herramienta rsync ofrece mecanismos desarrollados específicamente para transmitir sólo los cambios producidos dentro de los archivos. Esto no es aplicable únicamente a los archivos de texto, sino también a los binarios. Para detectar las diferencias entre los archivos, rsync los subdivide en bloques y procesa sus sumas de control.

El esfuerzo que implica la detección de los cambios tiene un precio. Es preciso ampliar de manera significativa los sistemas que se pretenden sincronizar mediante rsync; sobre todo en lo que respecta a la memoria RAM.

27.1.6 Novell iFolder

Novell iFolder permite acceder a los archivos desde cualquier ubicación y en todo momento. Al colocar archivos en un directorio de iFolder, se sincronizan instantáneamente con el servidor. Con este método, puede trabajar desde cualquier lugar.

Novell iFolder también permite trabajar sin conexión. Esto resulta muy cómodo si no dispone de conexión a Internet, por ejemplo al trabajar con un portátil cuando se encuentra de viaje. Después de establecer correctamente la conexión a Internet, los cambios realizados en el trabajo se envían al servidor.

El trabajo con iFolder implica los siguientes pasos:

1. Inicie sesión antes de trabajar con iFolder.
2. Modifique las preferencias de frecuencia de sincronización.
3. Sincronice los archivos y observe la actividad entre el cliente y el servidor de iFolder.
4. Resuelva los conflictos que se produzcan durante la sincronización. Los conflictos se producen cuando se modifica el mismo archivo en dos equipos diferentes. iFolder almacena los archivos en conflicto en un directorio distinto para evitar la pérdida de datos.

Para obtener más información acerca de iFolder, acceda a http://www.novell.com/en-en/documentation/. Encontrará sugerencias y trucos para iFolder en http://www.novell.com/coolsolutions/ifmag/.

27.2 Factores determinantes para seleccionar un programa

Hay algunos factores importantes que se deben tener en cuenta al decidir el programa que desea utilizar.

27.2.1 Comparación entre la estructura de cliente y servidor y la de par a par

Normalmente se utilizan dos modelos diferentes para la distribución de datos. En el primer modelo, todos los clientes sincronizan sus archivos con un servidor central. Todos los clientes deben tener acceso al servidor, al menos ocasionalmente. Este es el modelo que utilizan Subversion, CVS y WebDAV.

La otra posibilidad es permitir que todos los hosts en red sincronicen sus datos entre ellos como pares. Este es el concepto que rige el funcionamiento de Unison. rsync funciona como un cliente, pero cualquier cliente puede actuar también como servidor.

27.2.2 Portabilidad

Subversion, CVS y Unison también están disponibles para muchos otros sistemas operativos, incluidas varias versiones de Unix y Windows.

27.2.3 Interacción y automatización

En Subversion, CVS, WebDAV y Unison, el usuario debe iniciar manualmente la sincronización de datos. Esto permite un control preciso sobre los datos que se deben sincronizar y una gestión sencilla de los conflictos. No obstante, si los intervalos de sincronización son demasiado largos, es más probable que se produzcan conflictos.

27.2.4 Conflictos: incidencias y soluciones

En Subversion y CVS no suelen producirse conflictos, incluso cuando varias personas trabajan en un proyecto grande. Este hecho se debe a que los documentos se fusionan basándose en líneas individuales. Cuando se produce un conflicto, sólo resulta afectado un cliente. Normalmente resulta muy sencillo resolver los conflictos en Subversion y CVS.

Unison informa de los conflictos y permite excluir los archivos afectados de la sincronización. No obstante, los cambios no pueden fusionarse de forma tan sencilla como en Subversion o CVS.

A diferencia de Subversion y CVS, que permiten aceptar cambios parciales en caso de conflicto, WebDAV sólo lleva a cabo una comprobación cuando la modificación completa se considera correcta.

rsync no ofrece funciones de gestión de conflictos. El usuario es el responsable de no sobrescribir archivos por error y de resolver manualmente todos los posibles conflictos. Para aumentar la seguridad, puede emplearse como complemento un sistema de versiones (por ejemplo, RCS).

27.2.5 Selección y adición de archivos

En su configuración estándar, Unison sincroniza un árbol de directorios completo. Los archivos nuevos que aparecen en el árbol se incluyen automáticamente en la sincronización.

En Subversion y en CVS, los nuevos directorios y archivos se deben añadir de forma explícita mediante los comandos `svn add` o `cvs add`, respectivamente. Gracias a esto, aumenta el control del usuario sobre los archivos que desea sincronizar. Por otra parte, a menudo el usuario omite por error los archivos nuevos, especialmente cuando no se da cuenta de los signos de interrogación al consultar los resultados de `svn update` y `svn status` o `cvs update`, debido al gran número de archivos.

27.2.6 Histórico

Una función adicional de Subversion y CVS es que permiten reconstruir versiones antiguas de los archivos. Existe la posibilidad de introducir una nota de edición breve

para cada cambio, lo que facilita la tarea de seguimiento del desarrollo de los archivos, a partir del contenido y de las notas. Esta función es de gran ayuda para las tesis y los códigos de programación.

27.2.7 Volumen de los datos y requisitos de disco duro

Es necesario disponer de la cantidad de espacio libre suficiente para todos los datos distribuidos en los discos duros de todos los hosts implicados. Subversion y CVS requieren espacio adicional en el servidor para la base de datos de repositorio. El historial de archivos también se almacena en el servidor, lo que requiere más espacio. Cuando se modifican los archivos en formato de texto, sólo es necesario guardar las líneas modificadas. Los archivos binarios requieren un espacio adicional equivalente al tamaño total del archivo cada vez que sufren una modificación.

27.2.8 GUI

Unison ofrece una interfaz gráfica de usuario que muestra los procedimientos de sincronización que Unison sugiere realizar. Acepte las propuestas o excluya los archivos individuales de la sincronización. En el modo de texto, confirme de forma interactiva los procedimientos individuales.

Los usuarios experimentados suelen ejecutar Subversion y CVS desde la línea de comandos. No obstante, existen interfaces gráficas disponibles para Linux, como cervisia, y para otros sistemas operativos, como wincvs. Muchas herramientas de desarrollo, como kdevelop y editores de texto, como emacs, proporcionan soporte para CVS y Subversion. Normalmente, la resolución de conflictos resulta mucho más sencilla de llevar a cabo con estas interfaces.

27.2.9 Facilidad de uso

Unison y rsync son herramientas bastante sencillas de utilizar y muy adecuadas para usuarios sin experiencia. CVS y Subversion son un tanto más difíciles de utilizar. Los usuarios deben entender la interacción entre el repositorio y los datos locales. Los cambios en los datos deben fusionarse primero localmente con el repositorio. Esta acción se lleva a cabo mediante el comando `cvs update` o `svn update`. A conti-

nuación, deben enviarse los datos de vuelta al repositorio con el comando `cvs commit` o `svn commit`. Una vez entendido este procedimiento, los usuarios recién llegados también podrán utilizar CVS y Subversion fácilmente.

27.2.10 Seguridad contra los ataques

Durante las transmisiones, lo idóneo sería que los datos estuvieran protegidos contra posibles intercepciones y manipulaciones. Unison, CVS, rsync y Subversion pueden utilizarse de forma sencilla mediante ssh (shell segura), lo que proporciona seguridad contra ataques de esta clase. Debe evitarse la ejecución de CVS y Unison mediante rsh (shell remota). Tampoco es aconsejable acceder a CVS con el mecanismo *pserver* en redes no seguras. Subversion proporciona las medidas de seguridad necesarias al ejecutarse con Apache.

27.2.11 Protección contra las pérdidas de datos

Los desarrolladores llevan mucho tiempo utilizando CVS para gestionar proyectos de programación, por lo que es una herramienta muy estable. Dado que el historial de desarrollo se almacena, CVS proporciona protección incluso contra algunos errores de los usuarios, como la supresión accidental de un archivo. Aunque Subversion no es tan común como CVS, ya se emplea en entornos de producción (por ejemplo, en el propio proyecto de Subversion).

Unison es aún relativamente reciente, pero incorpora un gran nivel de estabilidad. No obstante, es más vulnerable a los errores de los usuarios. Una vez que se ha confirmado la sincronización de la supresión de un archivo, no existe ninguna posibilidad de restaurar el archivo.

Tabla 27.1 *Funciones de las herramientas de sincronización de archivos: -- = muy pobre, - = pobre o no disponible, o = media, + = buena, ++ = excelente, x = disponible*

	Unison	**CVS/SVN**	**rsync**	**mailsync**
Cliente/servidor	igual	C-S/C-S	C-S	igual

	Unison	CVS/SVN	rsync	mailsync
Portabilidad	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x
Interactividad	x	x/x	x	-
Velocidad	-	o/+	+	+
Conflictos	o	++/++	o	+
Sel. arch.	Dir.	Sel. arch., dir.	Dir.	Buzón
Histórico	-	x/x	-	-
Espacio en el disco duro	o	--	o	+
GUI	+	o/o	-	-
Dificultad	+	o/o	+	o
Ataques	+(ssh)	+/+(ssh)	+(ssh)	+(SSL)
Pérdidas de datos	+	++/++	+	+

27.3 Introducción a Unison

Unison es una solución excelente para la sincronización y transferencia de árboles de directorios completos. La sincronización se lleva a cabo en ambas direcciones y puede controlarse mediante una interfaz gráfica muy intuitiva. También se puede utilizar una versión de consola de texto. La sincronización puede automatizarse para que la interacción con el usuario no sea obligatoria, pero se necesita experiencia.

27.3.1 Requisitos

Unison debe estar instalado tanto en el cliente como en el servidor. En este contexto, el término *servidor* hace referencia a un segundo host remoto (a diferencia de CVS, que se describe en la Sección 27.1.2, “CVS” (p. 526)).

En la siguiente sección, Unison se utiliza junto a ssh. En este caso, se debe instalar un cliente SSH en el cliente y un servidor SSH en el servidor.

27.3.2 Uso de Unison

El enfoque que emplea Unison es la asociación de dos directorios (*raíces*) entre ellos. Esta asociación es simbólica, no es una conexión en línea. En este ejemplo, la distribución de directorios es la siguiente:

Cliente:	`/home/tux/dir1`
Servidor:	`/home/geeko/dir2`

Desea sincronizar estos dos directorios. El nombre del usuario es tux en el cliente y `geeko` en el servidor. En primer lugar, hay que comprobar si funciona la comunicación entre el cliente y el servidor:

```
unison -testserver /home/tux/dir1 ssh://geeko@server//homes/geeko/dir2
```

Los problemas que se producen con mayor frecuencia son los siguientes:

- Las versiones de Unison del cliente y del servidor no son compatibles.
- El servidor no permite las conexiones SSH.
- Ninguna de las dos vías especificadas existe.

Si todo funciona, omita la opción `-testserver`. Durante la primera sincronización, Unison aún no conoce la relación entre ambos directorios y envía sugerencias sobre la dirección de transferencia de los archivos y directorios individuales. Las flechas de la columna *Action* (Acción) indican la dirección de transferencia. Un signo de interrogación significa que Unison no puede realizar una sugerencia sobre la dirección de transferencia porque ambas versiones son nuevas o han sido modificadas.

Las teclas de flecha se pueden utilizar para establecer la dirección de transferencia de las entradas individuales. Si las direcciones de transferencia son correctas para todas las entradas que aparecen, haga clic en *Go* (Ir).

Las características de Unison (por ejemplo, la capacidad de efectuar la sincronización automáticamente en los casos evidentes) puede controlarse mediante parámetros de la línea de comandos especificados al iniciar el programa. Utilice el comando `unison --help` para ver la lista completa de parámetros.

Ejemplo 27.1 *El archivo ~/.unison/example.prefs*

```
root=/home/tux/dir1
root=ssh://wilber@server//homes/wilber/dir2
batch=true
```

Para cada par se mantiene un registro de sincronización en el directorio de usuario `~/.unison`. Los conjuntos de configuraciones, como `~/.unison/example.prefs`, también se pueden almacenar en este directorio. Para iniciar la sincronización, especifique este archivo como parámetro de línea de comandos, como en `unison example.prefs`.

27.3.3 Información adicional

La documentación oficial de Unison resulta muy útil. Por este motivo, esta sección simplemente proporciona una breve introducción. El manual completo está disponible en `http://www.cis.upenn.edu/~bcpierce/unison/` y en el paquete `unison` de SUSE.

27.4 Introducción a CVS

CVS es una herramienta adecuada para tareas de sincronización si los archivos individuales se editan con mucha frecuencia y se almacenan en un formato de archivo como texto ASCII o texto de código fuente. Es posible el uso de CVS para sincronizar los datos de otros formatos, como archivos JPEG, pero genera grandes cantidades de datos, ya que todas las variantes de cada archivo se almacenan de forma permanente en el servidor CVS. En esos casos, no es posible utilizar muchas de las posibilidades de CVS. La utilización de CVS para sincronizar archivos sólo es posible si todas las estaciones de trabajo pueden acceder al mismo servidor.

27.4.1 Configuración de un servidor CVS

El *servidor* es el host en el que se encuentran todos los archivos válidos, incluidas las versiones más recientes de todos los archivos. Cualquier estación de trabajo fija puede utilizarse como servidor. Si es posible, los datos del repositorio CVS deben incluirse en copias de seguridad regulares.

Al configurar un servidor CVS, puede ser buena idea proporcionar a los usuarios acceso al servidor mediante SSH. Si el nombre del usuario en el servidor es `tux` y el software CVS está instalado tanto en el cliente como en el servidor, será necesario definir las siguientes variables de entorno en el cliente:

```
CVS_RSH=ssh CVS_ROOT=tux@server:/serverdir
```

Puede utilizar el comando `cvs init` para iniciar el servidor CVS desde el cliente. Sólo es necesario llevar a cabo esta acción una vez.

Por último, es necesario asignar un nombre a la sincronización. Seleccione o cree un directorio en el cliente, exclusivamente para que contenga los archivos que desea gestionar con CVS (el directorio puede estar vacío). El nombre del directorio será también el de la sincronización. En este ejemplo, el directorio se llama `synchome`. Acceda a este directorio e introduzca los siguientes comandos para establecer `synchome` como nombre de la sincronización:

```
cvs import synchome tux wilber
```

Muchos comandos de CVS requieren un comentario. Para que sea posible incluirlo, CVS inicia un editor (el editor definido en la variable de entorno `$EDITOR` o vi si no se ha definido ninguno). El editor puede eludirse introduciendo el comentario antes de la línea de comandos, como en el siguiente ejemplo:

```
cvs import -m "esto es una prueba" synchome tux wilber
```

27.4.2 Uso de CVS

El repositorio de sincronización puede consultarse desde todos los hosts con el comando `cvs co synchome`. Esta acción crea un nuevo subdirectorio `synchome` en el cliente. Para asignar los cambios al servidor, acceda al directorio `synchome` (o uno de sus subdirectorios) e introduzca `cvs commit`.

Por defecto, todos los archivos (incluidos los subdirectorios) se asignan al servidor. Para asignar únicamente archivos o directorios individuales, especifíquelos de la siguiente forma: `cvs commit archivo1 directorio1`. Los archivos y directorios nuevos deben añadirse primero al repositorio con el comando `cvs add archivo1 directorio1` para que sea posible asignarlos al servidor. A continuación, asigne los archivos y directorios recién añadidos con `cvs commit archivo1 directorio1`.

Si cambia a otra estación de trabajo, compruebe el repositorio de sincronización, si no lo ha hecho ya durante una sesión anterior en la misma estación de trabajo (consulte el procedimiento descrito anteriormente).

Inicie la sincronización con el servidor mediante `cvs update`. Actualice los archivos o directorios individuales con el comando `cvs update archivo1 directorio1`. Para observar las diferencias entre los archivos actuales y las versiones almacenadas en el servidor, utilice el comando `cvs diff` o `cvs diff archivo1 directorio1`. Utilice `cvs -nq update` para conocer los archivos que resultarían afectados por una actualización.

A continuación encontrará algunos de los símbolos de estado que aparecen durante las actualizaciones:

U
: Se ha actualizado la versión local. Esto afecta a todos los archivos proporcionados por el servidor que faltan en el sistema local.

M
: Se ha modificado la versión local. Si se han producido cambios en el servidor, ha sido posible fusionar las diferencias en la copia local.

P
: Se ha revisado la versión local con la versión del servidor.

C
: El archivo local está en conflicto con la versión actual del repositorio.

?
: El archivo no existe en CVS.

El estado `M` indica un archivo modificado localmente. Asigne la copia local al servidor o elimine el archivo local y vuelva a ejecutar la actualización. El archivo que falta se recuperará del servidor. Si asigna un archivo modificado localmente y el archivo ha

sido modificado en la misma línea y asignado, puede producirse un conflicto, indicado con el símbolo de estado `C`.

Si se da el caso, busque las marcas de conflicto (»> y «<) en el archivo y decida entre las dos versiones. Dado que esta tarea puede resultar tediosa, puede decidir si desea desechar los cambios, suprimir el archivo local e introducir `cvs up` para recuperar la versión actual del servidor.

27.4.3 Información adicional

Esta sección simplemente ofrece una breve introducción a las muchas posibilidades de CVS. Encontrará una documentación más completa en las siguientes direcciones URL:

```
http://www.cvshome.org/
http://www.gnu.org/manual/
```

27.5 Introducción a Subversion

Subversion es un sistema de control de versiones de código abierto que se suele considerar sucesor de CVS, lo que significa que las funciones ya introducidas en CVS normalmente también se encuentran en Subversion. Resulta especialmente recomendable si busca las ventajas de CVS pero no quiere sufrir sus inconvenientes. Muchas de estas funciones ya se han presentado brevemente en la Sección 27.1.3, “Subversion” (p. 527).

27.5.1 Instalación de un servidor de Subversion

La instalación de una base de datos de repositorio en un servidor es un procedimiento relativamente sencillo. Subversion proporciona una herramienta de administración dedicada a este fin. El comando que debe introducir para crear un nuevo repositorio es el siguiente:

```
svnadmin create /vía/a/repositorio
```

Utilice `svnadmin help` para acceder a una lista de opciones adicionales. A diferencia de CVS, Subversion no se basa en RCS, sino en distintos tipos de repositorios. Se suelen utilizar los sistemas Berkeley Database o FSFS (un repositorio que utiliza el sistema

de archivos directamente). No instale un repositorio en sistemas de archivos remotos, como NFS, AFS o Windows SMB. La base de datos requiere mecanismos de bloqueo POSIX, que no son compatibles con estos sistemas de archivos.

El comando `svnlook` proporciona información sobre un repositorio existente.

```
svnlook info /vía/a/repositorio
```

Deberá configurar un servidor para permitir el acceso al repositorio a distintos tipos de usuarios. Para ello, utilice el servidor Web Apache con WebDAV, o bien svnserve, el servidor incluido en el paquete de Subversion. Cuando svnserve esté en funcionamiento, se podrá acceder al repositorio mediante una dirección URL con `svn://` o `svn+ssh://`. Los usuarios que deben autenticarse al llamar a `svn` pueden definirse en `/etc/svnserve.conf`.

Decidir entre Apache y svnserve depende de muchos factores. Es recomendable consultar el manual de Subversion. Encontrará más información en la Sección 27.5.3, "Información adicional" (p. 541).

27.5.2 Uso y funcionamiento

Utilice el comando `svn` (similar a `cvs`) para acceder a un repositorio de Subversion. Con `svn help` obtendrá la descripción de un parámetro de comando:

```
checkout (co): Check out a working copy from a repository.
usage: checkout URL[@REV]... [PATH]

  If specified, REV determines in which revision the URL is first
  looked up.

  If PATH is omitted, the basename of the URL will be used as
  the destination. If multiple URLs are given each will be checked
  out into a sub-directory of PATH, with the name of the sub-directory
  being the basename of the URL.
...
```

Cualquier cliente puede acceder al contenido proporcionado por un servidor configurado de forma correcta con el repositorio correspondiente, empleando uno de los siguientes comandos:

```
svn list http://svn.ejemplo.com/vía/a/proyecto
```

O bien

```
svn list svn://svn.ejemplo.com/vía/a/proyecto
```

Utilice el comando `svn checkout` para guardar un proyecto existente en el directorio actual:

```
svn checkout http://svn.ejemplo.com/vía/a/proyecto nombredelproyecto
```

Esta acción crea un nuevo subdirectorio `nombredelproyecto` en el cliente. A partir de este momento, podrá realizar operaciones en él (adiciones, copias, cambios de nombres y supresiones):

```
svn add archivo
svn copy archivoanterior archivonuevo
svn move archivoanterior archivonuevo
svn delete archivo
```

Estos comandos también pueden utilizarse sobre directorios. Subversion también puede guardar las propiedades de un archivo o directorio:

```
svn propset license GPL foo.txt
```

El ejemplo anterior establece el valor `GPL` para la propiedad `license` (Licencia). Utilice `svn proplist` para mostrar las propiedades:

```
svn proplist --verbose foo.txt
 Properties on 'foo.txt':
 license : GPL
```

Utilice `svn commit` para guardar los cambios en el servidor. Los demás usuarios podrán incorporar los cambios a sus directorios de trabajo al efectuar la sincronización con el servidor mediante `svn update`.

A diferencia de CVS, en Subversion se puede ver el estado de un directorio de trabajo *sin* acceder al repositorio, con el comando `svn status`. Los cambios locales aparecen en cinco columnas, de las cuales la primera es la más importante:

' '
: Sin cambios.

'A'
: Objeto marcado para su adición.

'D'
: Objeto marcado para su supresión.

'M'
: Objeto modificado.

'C'
: Objeto en conflicto.

'I'
: Objeto omitido.

'?'
: Objeto no mantenido por el control de versiones.

'!'
: Se ha informado de que el objeto no se encuentra. Este indicador aparece cuando el objeto se suprime o mueve sin utilizar el comando `svn`.

'~'
: El objeto se mantenía como archivo, pero ha sido sustituido por un directorio, o viceversa.

La segunda columna muestra el estado de las propiedades. Puede consultar el significado de las demás columnas en el manual de Subversion.

27.5.3 Información adicional

El primer punto de referencia es la página del proyecto Subversion en la siguiente dirección: `http://subversion.tigris.org/`. Después de instalar el paquete `subversion-doc`, encontrará un libro muy recomendable en el directorio `file:///usr/share/doc/packages/subversion/html/book.html` (también se encuentra disponible en línea en la siguiente dirección: `http://svnbook.red-bean.com/svnbook/index.html`).

27.6 Introducción a rsync

rsync resulta útil cuando es necesario transmitir grandes cantidades de datos regularmente sin realizar demasiados cambios. Este caso se da muy a menudo, por ejemplo, al crear copias de seguridad. Otra aplicación está relacionada con los servidores temporales. Se trata de servidores que almacenan árboles de directorios completos de servidores Web que se duplican regularmente en un servidor Web de una zona DMZ.

27.6.1 Configuración y funcionamiento

rsync puede funcionar de dos modos diferentes. Puede utilizarse para crear archivos de reserva o copiar datos. Para ello, sólo es necesario disponer de una shell remota, como ssh, en el sistema de destino. No obstante, rsync también puede utilizarse como `daemon` para proporcionar directorios a la red.

El modo básico de funcionamiento de rsync no requiere ninguna configuración especial. rsync permite la duplicación directa de directorios completos en otro sistema. A modo de ejemplo, el siguiente comando crea una copia de seguridad del directorio personal de tux en un servidor de copias de seguridad llamado sun:

```
rsync -baz -e ssh /home/tux/ tux@sun:backup
```

El siguiente comando se utiliza para recuperar el directorio:

```
rsync -az -e ssh tux@sun:backup /home/tux/
```

Hasta este punto, la gestión no se diferencia mucho de la de una herramienta de copia normal, como scp.

rsync debe utilizarse en el modo de "rsync" para que todas sus funciones estén totalmente disponibles. Para ello, es necesario iniciar el daemon rsyncd en uno de los sistemas. Configúrelo en el archivo `/etc/rsyncd.conf`. Por ejemplo, para que el directorio `/srv/ftp` esté disponible con rsync, utilice la siguiente configuración:

```
gid = nobody
uid = nobody
read only = true
use chroot = no
transfer logging = true
log format = %h %o %f %l %b
log file = /var/log/rsyncd.log

[FTP]
        path = /srv/ftp
        comment = Un ejemplo
```

A continuación, inicie rsyncd mediante el comando `rcrsyncd start`. rsyncd también puede iniciarse automáticamente durante el proceso de arranque. Para ello, active este servicio en el editor de tiempo de ejecución proporcionado por YaST, o bien introduzca manualmente el comando `insserv rsyncd`. Como alternativa, xinetd también puede iniciar rsyncd. No obstante, esto sólo es recomendable para servidores que utilicen rsyncd con poca frecuencia.

El ejemplo también crea un archivo de registro que detalla todas las conexiones. Dicho archivo se almacena en `/var/log/rsyncd.log`.

A continuación podrá probar la transferencia desde un sistema cliente. Para ello, emplee el siguiente comando:

```
rsync -avz sun::FTP
```

Este comando proporciona una lista de todos los archivos que se encuentran en el directorio `/srv/ftp` del servidor. Esta solicitud también se incluye en el archivo de registro `/var/log/rsyncd.log`. Para iniciar una transferencia real, proporcione un directorio de destino. Utilice `.` para el directorio actual. Por ejemplo:

```
rsync -avz sun::FTP .
```

Por defecto, no se suprime ningún archivo al realizar la sincronización mediante rsync. Si es necesario forzar la supresión, deberá definir la opción adicional `--delete`. Para asegurarse de que no se suprime ningún archivo reciente en lugar de uno antiguo, puede utilizar la opción `--update` en lugar de la anterior. Deberá resolver manualmente cualquier conflicto que se produzca.

27.6.2 Información adicional

En las páginas Man `man rsync` y `man rsyncd.conf` encontrará información importante sobre rsync. En `/usr/share/doc/packages/rsync/tech_report.ps` encontrará un documento técnico de referencia sobre los principios del funcionamiento de rsync. Para conocer las noticias más recientes sobre rsync, visite la página Web del proyecto en la siguiente dirección: http://rsync.samba.org/.

27.7 Introducción a mailsync

mailsync resulta especialmente adecuado para las tres tareas siguientes:

- Sincronización de mensajes de correo electrónico almacenados localmente con los almacenados en un servidor
- Migración de buzones de correo a un formato diferente o a un servidor diferente
- Comprobación de la integridad de un buzón de correo o búsqueda de duplicados

27.7.1 Configuración y uso

mailsync distingue entre el propio buzón de correo (el *almacén*) y la conexión entre ambos buzones (el *canal*). Las definiciones de los almacenes y los canales se guardan en `~/.mailsync`. Los siguientes párrafos explican varios ejemplos de almacenes.

Una definición sencilla puede tener la siguiente estructura:

```
store saved-messages {
   pat Mail/saved-messages
prefix  Mail/
}
```

`Mail/` es un subdirectorio del directorio personal del usuario que contiene carpetas de correo electrónico, incluida la carpeta `saved-messages`. Si mailsync se inicia mediante el comando `mailsync -m saved-messages`, muestra un índice de todos los mensajes de `saved-messages`. Si se realiza la siguiente definición:

```
store localdir {
pat     Mail/*
prefix  Mail/
}
```

el comando `mailsync -m localdir` muestra todos los mensajes incluidos en `Mail/`. Por el contrario, el comando `mailsync localdir` muestra los nombres de las carpetas. Las especificaciones de un almacén en un servidor IMAP presentan la siguiente estructura:

```
store imapinbox {
server {mail.edu.harvard.com/user=gulliver}
ref    {mail.edu.harvard.com}
pat    INBOX
}
```

El ejemplo anterior afecta únicamente a la carpeta principal del servidor IMAP. Un almacén para las subcarpetas tendría la siguiente estructura:

```
store imapdir {
server {mail.edu.harvard.com/user=gulliver}
ref {mail.edu.harvard.com}
pat INBOX.*
prefix  INBOX.
}
```

Si el servidor IMAP es compatible con las conexiones cifradas, la especificación del servidor debe modificarse del siguiente modo:

```
server {mail.edu.harvard.com/ssl/user=gulliver}
```

o bien, si el certificado del servidor no es conocido, del siguiente modo:

```
server {mail.edu.harvard.com/ssl/novalidate-cert/user=gulliver}
```

El prefijo se explicará a continuación.

Ahora las carpetas bajo `Mail/` deberían estar conectadas a los subdirectorios del servidor IMAP:

```
channel folder localdir imapdir {
msinfo .mailsync.info
}
```

mailsync utiliza el archivo `msinfo` para realizar un seguimiento de los mensajes ya sincronizados.

El comando `mailsync folder` hace lo siguiente:

- Amplía el patrón del buzón de correo en ambos lados.
- Elimina el prefijo de los nombres de carpetas resultantes.
- Sincroniza las carpetas por parejas (o las crea si no existían).

En consecuencia, la carpeta `INBOX.sent-mail` del servidor IMAP se sincroniza con la carpeta local `Mail/sent-mail` (siempre y cuando existan las definiciones explicadas anteriormente). La sincronización entre las carpetas individuales se lleva a cabo del modo siguiente:

- Si un mensaje ya existe en ambos lados, no ocurre nada.
- Si el mensaje no se encuentra en uno de los lados y es nuevo (no aparece en el archivo `msinfo`), se transmite a dicho lado.
- Si el mensaje sólo existe en un lado y es antiguo (aparece en el archivo `msinfo`), se suprime (porque el mensaje que existía en el otro lado también se ha suprimido).

Para saber por adelantado los mensajes que se transmitirán y los que se suprimirán durante la sincronización, inicie mailsync con un canal *y* un almacén, mediante el comando `mailsync folder localdir`. Este comando produce una lista de todos los mensajes nuevos del host local, así como de los mensajes que se suprimirían en el lado del IMAP durante la sincronización. Del mismo modo, el comando

`mailsync folder imapdir` produce una lista de todos los mensajes que son nuevos en el lado del IMAP, así como de los mensajes que se suprimirían en el host local durante la sincronización.

27.7.2 Problemas posibles

Si se producen pérdidas de datos, el método de recuperación más seguro es suprimir el archivo de registro de canal relevante `msinfo`. En consecuencia, todos los mensajes que sólo existan en un lado se considerarán nuevos y, por lo tanto, se transmitirán durante la próxima sincronización.

En la sincronización sólo se incluyen los mensajes con identificador. Los mensajes que no tienen identificador simplemente se omiten, lo que significa que no se transmiten ni suprimen. Las faltas de identificadores suelen ser provocadas por errores de los programas al enviar o escribir un mensaje.

En algunos servidores IMAP, se hace referencia a la carpeta principal con el nombre de `INBOX` y a las subcarpetas con nombres seleccionados aleatoriamente (lo que contrasta con la estructura INBOX e INBOX.nombre). Por lo tanto, en el caso de dichos servidores IMAP, no es posible especificar un patrón exclusivo para las subcarpetas.

Cuando se han transmitido correctamente los mensajes a un servidor IMAP, los controladores del buzón de correo (c-client) utilizados por mailsync establecen un indicador especial de estado. Por este motivo, algunos programas de correo electrónico, como mutt, no pueden reconocer estos mensajes como nuevos. Inhabilite el ajuste de este indicador especial de estado con la opción `-n`.

27.7.3 Información adicional

El archivo `README` (LÉAME) de `/usr/share/doc/packages/mailsync/`, incluido en `mailsync`, proporciona información adicional. A este respecto, la petición de comentario (RFC) 2076, “Common Internet Message Headers” (Encabezados de mensajes comunes de Internet), resulta especialmente interesante.

28 Samba

Mediante Samba, se puede configurar una máquina Unix como servidor de impresión y archivos para máquinas DOS, Windows y OS/2. Samba se ha desarrollado hasta convertirse en un producto maduro y más bien complejo. Samba se puede configurar con YaST, SWAT (interfaz de Web) o el archivo de configuración.

28.1 Terminología

Protocolo SMB
: Samba utiliza el protocolo SMB (Server Message Block, bloque de mensajes de servidor), que está basado en los servicios NetBIOS. Debido a las presiones de IBM, Microsoft liberó el protocolo para que otros fabricantes de software pudieran establecer conexiones con una red de dominio de Microsoft. Con Samba, el protocolo SMB funciona por encima del protocolo TCP/IP, de manera que éste último debe estar instalado en todos los clientes.

Protocolo CIFS
: CIFS (Common Internet File System, sistema de archivos comunes de Internet) es otro de los protocolos compatibles con Samba. CIFS define un protocolo estándar de acceso a sistemas de archivos remotos para su uso en la red, con lo que hace posible que grupos de usuarios trabajen juntos y compartan documentos a través de la red.

NetBIOS
: NetBIOS es una interfaz de software (API) diseñada para la comunicación entre máquinas. En él se ofrece un servicio de nombres que permite que las máquinas

conectadas a la red reserven nombres para ellas mismas. Tras la reserva, es posible dirigirse a las máquinas mediante el nombre. No existe ningún proceso central que compruebe los nombres. Cualquier máquina de la red puede reservar tantos nombres como desee, siempre que no estén ya en uso. La interfaz NetBIOS puede implementarse para diferentes arquitecturas de red. Una implementación que funciona de un modo relativamente próximo al hardware de red es NetBEUI, aunque a menudo se habla de ella como NetBIOS. Los protocolos implementados con NetBIOS son IPX de Novell (NetBIOS sobre TCP/IP) y TCP/IP.

Los nombres de NetBIOS enviados mediante TCP/IP no tienen nada en común con los nombres que se usan en `/etc/hosts/` o los definidos por DNS. NetBIOS utiliza su propia convención para la nomenclatura, completamente independiente. Sin embargo, es recomendable utilizar nombres que se correspondan con los nombres de host DNS para que la administración sea más sencilla. Esta es la opción que Samba utiliza por defecto.

Servidor Samba
: El servidor Samba es un servidor que proporciona servicios SMB/CIFS y NetBIOS a través de los servicios de nombre IP a los clientes. En Linux, existen dos daemons que corresponden al servidor Samba: smnd para los servicios SMB/CIFS y nmbd para los servicios de nombre.

Cliente Samba
: El cliente Samba es un sistema que utiliza los servicios proporcionados por un servidor Samba a través del protocolo SMB. Todos los sistemas operativos habituales, como Mac OS X, Windows y OS/2, son compatibles con el protocolo SMB. El protocolo TCP/IP debe estar instalado en todos los ordenadores. Samba ofrece clientes para las distintas versiones de UNIX. Para Linux, existe un módulo del núcleo para SMB que permite integrar recursos SMB en el nivel de sistema de Linux. No es preciso ejecutar ningún daemon para el cliente Samba.

Recursos compartidos
: Los servidores SMB ofrecen espacio de hardware a sus clientes por medio de recursos compartidos. Estos recursos son las impresoras y directorios, con los subdirectorios correspondientes, que se encuentran en el servidor. Se exporta mediante un nombre y se puede acceder a él a través de dicho nombre. El nombre del recurso compartido se puede definir como se quiera, no tiene que corresponder al nombre del directorio de exportación. A las impresoras también se les asigna un nombre. Los clientes pueden acceder a la impresora por su nombre.

28.2 Inicio y detención de Samba

Se puede iniciar o detener el servidor Samba automáticamente durante el arranque o de forma manual. La directiva de inicio y detención forma parte de la configuración del servidor Samba de YaST que se describe en la Sección 28.3.1, “Configuración de un servidor Samba con YaST” (p. 549).

Para iniciar o detener los servicios Samba en ejecución con YaST, seleccione *Sistema → Editor de niveles de ejecución.* Desde la línea de comandos puede detener los servicios necesarios para Samba con `rcsmb stop y rcnmb stop` e iniciarlos con `rcnmb start y rcsmb start`.

28.3 Configuración de un servidor Samba

Un servidor Samba se puede configurar en SUSE Linux de dos modos diferentes: con YaST o manualmente. La configuración manual ofrece un nivel superior de detalle, pero carece de la comodidad de la interfaz gráfica de YaST.

28.3.1 Configuración de un servidor Samba con YaST

Para configurar un servidor Samba, inicie YaST y seleccione *Servicios de red → Servidor Samba.* Cuando se inicia el módulo por primera vez, se muestra el cuadro de diálogo *Instalación del servidor Samba,* donde se le solicita que tome algunas decisiones básicas en relación con la administración del servidor. Al final de la configuración, este cuadro de diálogo solicita la contraseña del usuario Root de Samba. Cuando se inicia el servidor posteriormente, aparece el cuadro de diálogo *Configuración del servidor Samba.*

El cuadro de diálogo *Instalación del servidor Samba* consta de dos pasos:

Nombre de grupo de trabajo o dominio
: En *Nombre de grupo de trabajo o dominio,* seleccione un nombre existente o introduzca uno nuevo y haga clic en *Siguiente.*

Tipo de servidor Samba
: En el siguiente paso, especifique si el servidor debe actuar como PDC y haga clic en *Siguiente.*

Puede cambiar todos los ajustes de *Instalación del servidor Samba* más adelante en el cuadro de diálogo *Configuración del servidor Samba,* por medio de la pestaña *Identidad.*

Durante el primer inicio del módulo del servidor Samba, el cuadro de diálogo *Configuración del servidor Samba* se muestra inmediatamente después del cuadro de diálogo *Instalación del servidor Samba.* Está compuesto por tres pestañas:

Inicio
: En la pestaña *Inicio,* puede definir el inicio del servidor Samba. Para iniciar el servicio cada vez que se arranque el sistema, seleccione *Durante el arranque.* Para activar el inicio manual, elija *Manualmente.* Para obtener más información acerca del inicio del servidor Samba, consulte la Sección 28.2, “Inicio y detención de Samba” (p. 549).

  En esta pestaña puede también abrir puertos en el cortafuegos. Para ello, seleccione *Puerto abierto en el cortafuegos.* Si tiene varias interfaces de red, seleccione la que corresponda a los servicios Samba haciendo clic en *Detalles del cortafuegos,* seleccionando la interfaz y haciendo clic en *Aceptar.*

Recursos compartidos
: En esta pestaña puede determinar los recursos compartidos de Samba que se deben activar. Hay algunos predefinidos, como los que corresponden a los directorios personales y las impresoras. Utilice *Cambiar estado* para cambiar entre *Activo* e *Inactive* (Inactivo). Haga clic en *Añadir* para agregar recursos compartidos nuevos o en *Suprimir* para eliminar el recurso compartido seleccionado.

Identity (Identidad)
: En la pestaña *Identidad,* puede determinar el dominio con el que está asociado el host (*Configuración básica*) y si se debe utilizar un nombre de host alternativo en la red (*Nombre de host de NetBIOS*). Para definir ajustes globales de experto o la autenticación de usuarios, haga clic en *Configuración avanzada.*

Haga clic en *Finalizar* para cerrar la configuración.

28.3.2 Administración Web con SWAT

SWAT (Samba Web Administration Tool, herramienta de administración Web de Samba) es una herramienta alternativa para administrar el servidor Samba. Este programa ofrece una interfaz Web sencilla que permite configurar el servidor Samba. Para utilizar SWAT, abra `http://localhost:901` en un navegador Web e inicie la sesión como usuario `Root`. Si no dispone de una cuenta de usuario Root especial para Samba, utilice la cuenta de usuario `Root` del sistema.

NOTA: Activación de SWAT

Después de la instalación del servidor Samba, SWAT no está activado. Para activarlo, abra *Servicios de red → Servicios de red (xinetd)* en YaST, habilite la configuración de los servicios de red, seleccione *swat* en la tabla y haga clic en *Cambiar estado* (encendido o apagado).

28.3.3 Configuración del servidor manualmente

Si tiene la intención de utilizar Samba como servidor, debe instalar `samba`. El archivo de configuración principal de Samba es `/etc/samba/smb.conf`. Este archivo se puede dividir en dos partes lógicas. La sección `[global]` contiene los ajustes centrales y globales. Las secciones `[share]` contienen cada uno de los recursos compartidos de archivos e impresión. De esta manera, los detalles se pueden configurar de manera diferente para cada recurso compartido o bien de manera global en la sección `[global]`, con lo que se mejora la transparencia del archivo de configuración.

La sección global

Para que las otras máquinas puedan acceder al servidor Samba por medio de SMB en un entorno Windows, deben ajustarse los siguientes parámetros de la sección `[global]` para que se adecuen a las necesidades de la configuración de la red.

workgroup = TUX-NET

Esta línea asigna el servidor Samba a un grupo de trabajo. Sustituya `TUX-NET` por el grupo de trabajo adecuado del entorno de red. El servidor Samba aparece bajo su nombre DNS, a menos que dicho nombre ya se haya asignado a otra máquina

de la red. Si el nombre DNS no está disponible, establezca el nombre del servidor mediante `netbiosname=MINOMBRE`. Consulte `mansmb.conf` para conocer más detalles de este parámetro.

os level = 2
: De este parámetro depende que el servidor Samba intente establecerse como LMB (Local Master Browser, navegador principal local) para el grupo de trabajo correspondiente. Seleccione un valor muy bajo para evitar que la red Windows existente se vea perturbada por un servidor Samba mal configurado. Podrá encontrar más información sobre este punto importante en los archivos `BROWSING.txt` y `BROWSING-Config.txt` del subdirectorio `textdocs` de la documentación del paquete.

  Si no existe ningún otro servidor SMB en la red (como servidores Windows NT o 2000) y desea que el servidor Samba lleve una lista de todos los sistemas disponibles en el entorno local, aumente el valor de `os level` (por ejemplo, hasta `65`). El servidor Samba se elegirá como LMB para la red local.

  Al cambiar este valor, tenga muy en cuenta cómo podría afectar a un entorno de red Windows existente. Pruebe los cambios primero en una red aislada o en momentos del día que no sean críticos.

wins support y wins server
: Para integrar el servidor Samba en una red Windows existente en la que haya un servidor WINS activo, active la opción `wins server` y establezca como su valor la dirección IP del servidor WINS.

  Si las máquinas Windows están conectadas a subredes separadas pero deben ser visibles entre sí, es necesario establecer un servidor WINS. Para convertir el servidor Samba en dicho servidor WINS, establezca la opción `wins support = Yes`. Asegúrese de que sólo un servidor de la red tiene este ajuste habilitado. Las opciones `wins server` y `wins support` no deben habilitarse nunca al mismo tiempo en el archivo `smb.conf`.

Recursos compartidos

En los siguientes ejemplos se indica cómo poner a disposición de los clientes SMB una unidad de CD-ROM y los directorios de usuario (`homes`).

[cdrom]
Para impedir la activación por error del acceso a la unidad de CD-ROM, las siguientes líneas se han desactivado mediante marcas de comentario (en este caso, puntos y coma). Elimine los puntos y coma de la primera columna para compartir la unidad de CD-ROM mediante Samba.

Ejemplo 28.1 *Un CD-ROM como recurso compartido*

```
;[cdrom]
;       comment = Linux CD-ROM
;       path = /media/cdrom
;       locking = No
```

`[cdrom]` y `comment`
La entrada `[cdrom]` es el nombre del recurso compartido que verán todos los clientes SMB de la red. De forma opcional, se puede añadir un `comment` para describir más detalladamente el recurso compartido.

`path = /media/cdrom`
`path` exporta el directorio `/media/cdrom`.

Mediante la restrictiva configuración por defecto, este tipo de recurso compartido sólo se encuentra disponible para usuarios presentes en el sistema. Si el recurso compartido debe estar disponible para todos los usuarios, añada la línea `guest ok = yes` a la configuración. Este ajuste concede permiso de lectura a todos los usuarios de la red. Se recomienda utilizarlo con mucho cuidado. En particular, hay que utilizarlo con mucho cuidad en la sección `[global]`.

`[homes]`
El recurso compartido `[home]` tiene una importancia especial. Si el usuario dispone de una cuenta válida y de una contraseña en el servidor de archivos Linux y de su propio directorio personal, podrá acceder a él.

Ejemplo 28.2 *Recurso compartido homes*

```
[homes]
 comment = Home Directories
 valid users = %S
 browseable = No
 read only = No
 create mask = 0640
 directory mask = 0750
```

[homes]
: Siempre y cuando no exista otro recurso compartido que utilice como nombre de recurso compartido el del usuario que se conecte al servidor SMB, se creará de forma dinámica un recurso compartido mediante las directivas de recurso compartido de `[homes]`. El nombre del recurso compartido que resulte será el nombre del usuario.

`valid users = %S`
: Una vez que la conexión quede correctamente establecida, %S se reemplazará por el nombre específico del recurso compartido. En el caso de un recurso compartido `[homes]`, éste será siempre del nombre del usuario. Como consecuencia, los derechos de acceso al recurso compartido de un usuario quedarán restringidos al propio usuario.

`browseable = No`
: Este ajuste hace que el recurso compartido no pueda verse en el entorno de red.

`read only = No`
: Por defecto, Samba deniega el permiso de escritura a todos los recursos compartidos exportados mediante el parámetro `read only = Yes`. Para tener permiso de escritura en un recurso compartido, establezca el valor `read only = No`, que es equivalente a `writeable = Yes`.

`create mask = 0640`
: Los sistemas no basados en MS Windows NT no comprenden el concepto de los permisos de UNIX, por lo que no pueden establecerlos al crear un archivo. El parámetro `create mask` define los permisos de acceso que se asignarán a los archivos de nueva creación. Esto sólo se aplica a los recursos compartidos en los que se puede escribir. En concreto, este ajuste significa que el propietario tiene permisos de lectura y escritura, y que los miembros del grupo primario del usuario tienen permisos de lectura. `valid users = %S` impide el acceso de lectura incluso aunque el grupo tenga permiso para ello. Para que el grupo tenga acceso de lectura y escritura, desactive la línea `valid users = %S`.

Nivel de seguridad

Es posible proteger el acceso a cada recurso compartido mediante una contraseña para aumentar la seguridad. SMB dispone de tres maneras posibles de comprobar los permisos:

Seguridad en el nivel del recurso compartido (security = share)
: Se asigna una contraseña fija al recurso compartido. Todos los que conozcan la contraseña tendrán acceso al recurso compartido.

Seguridad en el nivel del usuario (security = user)
: Esta variante introduce el concepto de usuario en SMB. Cada usuario debe registrarse en el servidor con su propia contraseña. Después del registro, el servidor puede dar acceso a cada recurso compartido exportado en función de los nombres de usuario.

Seguridad en el nivel del servidor (security = server):
: De cara a los clientes, Samba actúa como si trabajara en el modo de nivel de usuario. Sin embargo, todas las peticiones de contraseñas se pasan a otro servidor en modo de nivel de usuario, que es el encargado de la autenticación. Este ajuste requiere un parámetro adicional (`password server`).

La selección de la seguridad en el nivel del recurso compartido, del usuario o del servidor afecta al servidor entero. No es posible ofrecer ciertos recursos compartidos en la configuración de un servidor con seguridad en el nivel del recurso compartido y otros con seguridad en el nivel del usuario. No obstante, se puede ejecutar un servidor Samba individual para cada dirección IP configurada en el sistema.

Hay más información sobre este tema en el documento Samba HOWTO Collection. Para el caso de un solo sistema con varios servidores, estudie las opciones `interfaces` y `bind interfaces only`.

28.4 Configuración de los clientes

Los clientes sólo pueden acceder al servidor Samba mediante TCP/IP. NetBEUI y NetBIOS no se pueden utilizar mediante IPX con Samba.

28.4.1 Configuración de un cliente Samba con YaST

Configure un cliente Samba para acceder a recursos (archivos o impresoras) en el servidor Samba. Introduzca el dominio o el grupo de trabajo en el cuadro de diálogo *Grupo de trabajo SAMBA*. Haga clic en *Examinar* para ver todos los grupos y dominios

disponibles que se pueden seleccionar con el ratón. Si activa *Usar también la información SMB para la autentificación de Linux*, la autenticación de usuarios se realizará en el servidor Samba. Cuando haya introducido todos los ajustes, haga clic en *Finalizar* para completar la configuración.

28.4.2 Windows 9x y ME

Windows 9x y ME ya incorporan compatibilidad con TCP/IP. Sin embargo, ésta no se instala por defecto. Para añadir TCP/IP, vaya a *Control Panel → System* (Panel de control - Sistema) y escoja *Add → Protocols → TCP/IP from Microsoft* (Agregar - Protocolos - TCP/IP de Microsoft). Después de reiniciar la máquina Windows, busque el servidor Samba haciendo doble clic en el icono del escritorio correspondiente al entorno de red.

SUGERENCIA

Para utilizar una impresora en el servidor Samba, instale el controlador de impresión estándar o Apple-PostScript que corresponda a la versión de Windows. Se recomienda enlazarlo con la cola de impresión de Linux, que admite PostScript como formato de entrada.

28.5 Samba como servidor de inicio de sesión

En las redes en las que se encuentren en su mayoría clientes de Windows, a menudo es preferible que los usuarios se puedan registrar sólo mediante una cuenta válida y una contraseña. En una red basada en Windows, esta tarea la gestiona un servidor Windows NT configurado como controlador de dominio primario (PDC, del inglés Primary Domain Controller), aunque también se puede realizar a través de un servidor Samba. En el Ejemplo 28.3, “Sección global de smb.conf” (p. 557) se muestran las entradas que deben realizarse en la sección `[global]` de `smb.conf`.

Ejemplo 28.3 *Sección global de smb.conf*

```
[global]
       workgroup = TUX-NET
       domain logons = Yes
       domain master = Yes
```

Si para la verificación se utilizan contraseñas cifradas (éste es el ajuste por defecto en instalaciones bien mantenidas de MS Windows 9x, MS Windows NT 4.0 a partir del Service Pack 3 y productos posteriores), el servidor Samba debe poder gestionarlas. Esto lo permite la entrada `encrypt passwords = yes` de la sección `[global]` (en la versión 3 de Samba, es la opción por defecto). Además, es necesario cifrar las cuentas de usuario y las contraseñas en un formato admitido por Windows. Hágalo con el comando `smbpasswd -a nombre`. Cree la cuenta de dominio para los equipos, necesaria debido al concepto de dominio de Windows NT, mediante los siguientes comandos:

Ejemplo 28.4 *Configuración de una cuenta de máquina*

```
useradd nombredehost\$
       smbpasswd -a -m nombredehost
```

Con el comando `useradd` se añade un símbolo de dólar. El comando `smbpasswd` lo inserta automáticamente al utilizar el parámetro `-m`. El ejemplo comentado de configuración (`/usr/share/doc/packages/Samba/examples/smb.conf.SuSE`) contiene ajustes para que esta tarea se realice automáticamente.

Ejemplo 28.5 *Configuración automática de una cuenta de máquina*

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" \
       -s /bin/false %m\$
```

Para que Samba pueda ejecutar este guión correctamente, elija un usuario de Samba con los permisos de administrador necesarios. Para ello, seleccione un usuario y añádalo al grupo `ntadmin`. A continuación puede asignar el estatus de `Domain Admin` a todos los usuarios de dicho grupo Linux mediante el comando:

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

En el capítulo 12 del documento Samba HOWTO Collection, que se encuentra en `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`, se ofrece más información.

28.6 Información adicional

En la documentación digital hay disponible información detallada sobre Samba. Introduzca `apropos samba` en la línea de comandos para ver las páginas de manual o simplemente explore el directorio `/usr/share/doc/packages/samba`, si está instalada la documentación de Samba, para obtener más documentación en línea y ejemplos. En el subdirectorio `ejemplos`, se encuentra una configuración de ejemplo comentada (`smb.conf.SuSE`).

El documento Samba HOWTO Collection ofrecido por el equipo Samba incluye una sección de solución de problemas. Además, la sección V del documento contiene una guía paso a paso para la comprobación de la configuración. Puede acceder a este documento en `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`, una vez que haya instalado el paquete `samba-doc`.

29 Servidor alterno Squid

Squid es un caché alterno (proxy) muy utilizado en plataformas Linux y UNIX. Esto significa que almacena los objetos de Internet solicitados, como los datos de un servidor Web o FTP, en un equipo más cercano a la estación de trabajo que los solicita que el servidor original. En este capítulo se describe su configuración, los ajustes necesarios para que funcione, cómo configurar el sistema para que el servicio del alterno sea transparente, cómo recopilar estadísticas de uso de caché con la ayuda de programas como Calamaris y cachemgr y cómo filtrar contenido Web con squidGuard.

Squid actúa como caché alterno (proxy). Redirige las solicitudes de objetos de los clientes (en este caso, los navegadores Web) al servidor. Cuando los objetos solicitados llegan del servidor, los entrega al cliente y conserva una copia en el caché del disco duro. Una de las ventajas del almacenamiento en caché es que si varios clientes solicitan el mismo objeto, el servicio los puede proporcionar desde el caché del disco duro. De este modo, los clientes reciben los datos mucho más rápido que cuando tienen que obtenerlos desde Internet. Este procedimiento también reduce el tráfico de la red.

Además del almacenamiento en caché, Squid ofrece una amplia variedad de funciones, como la distribución de la carga en las jerarquías de los servidores alternos, la definición de estrictas listas de control de acceso para todos los clientes que accedan al alterno, el permiso o la denegación de acceso a páginas Web concretas (con la ayuda de otras aplicaciones) y la generación de estadísticas de las páginas Web visitadas con más frecuencia con el fin de evaluar los hábitos de navegación de los usuarios. Squid no es un alterno genérico. Normalmente sólo ejerce sus funciones con conexiones HTTP. También es compatible con los protocolos FTP, Gopher, SSL y WAIS, pero no es compatible con otros protocolos de Internet, como Real Audio, noticias o videoconferencia. Dado que Squid sólo es compatible con el protocolo UDP para proporcionar

comunicaciones entre diferentes cachés, muchos otros programas multimedia tampoco son compatibles.

29.1 Algunos aspectos de los cachés alternos

Squid puede utilizarse de varios modos diferentes como caché alterno. Si se combina con un cortafuegos, puede mejorar la seguridad. Se pueden utilizar varios alternos al mismo tiempo. También es posible determinar los tipos de objetos que deben almacenarse en caché y durante cuánto tiempo.

29.1.1 Squid y la seguridad

Existe la posibilidad de utilizar Squid con un cortafuegos para proteger las redes internas del exterior al utilizar un caché alterno. El cortafuegos deniega el acceso a los servicios externos a todos los clientes excepto a Squid. Todas las conexiones Web deben establecerse a través del alterno. Con esta configuración, Squid controla por completo el acceso Web.

Si la configuración del cortafuegos incluye una zona DMZ, el alterno debe funcionar en dicha zona. La Sección 29.5, “Configuración de un alterno transparente” (p. 572) describe cómo implementar un alterno *transparente*. Esto simplifica la configuración de los clientes, dado que en este caso no necesitan ninguna información sobre el alterno.

29.1.2 Cachés múltiples

Existe la posibilidad de configurar varias sesiones de Squid de modo que intercambien objetos entre sí. Se reduce así la carga total del sistema y aumentan las posibilidades de encontrar un objeto que ya exista en la red local. También es posible configurar jerarquías de caché, de modo que un caché pueda enviar solicitudes de objetos a cachés del mismo nivel o a cachés principales, de modo que los objetos se obtengan de otro caché de la red local o directamente desde el origen.

La selección de la topología adecuada para la jerarquía de caché es muy importante, dado que no es deseable aumentar el tráfico general de la red. En una red muy grande,

puede resultar conveniente configurar un servidor alterno para cada subred y conectarlos a un alterno principal, que a su vez esté conectado al caché alterno del proveedor de Internet.

Todas estas comunicaciones se gestionan mediante ICP (protocolo de caché de Internet), que se ejecuta sobre el protocolo UDP. Las transferencias de datos entre cachés se gestionan mediante HTTP (protocolo de transmisión de hipertexto) basado en TCP.

Para encontrar el servidor más adecuado desde el que obtener los objetos, cada caché envía una solicitud ICP a todos los alternos del mismo nivel. Éstos responden a las solicitudes mediante respuestas ICP con un código HIT si se detecta el objeto, o MISS si no es así. Si se detectan varias respuestas HIT, el servidor alterno decide desde qué servidor desea efectuar la descarga, dependiendo de factores como el caché que envió la respuesta más rápida o el que se encuentra más cerca. Si no se recibe ninguna respuesta satisfactoria, la solicitud se envía al caché principal.

SUGERENCIA

Para evitar la duplicación de objetos en diferentes cachés de la red, se emplean otros protocolos ICP, como CARP (protocolo de encaminamiento de matrices de cachés) o HTCP (protocolo de caché de hipertexto). Cuantos más objetos se mantengan en la red, mayores son las posibilidades de encontrar el deseado.

29.1.3 Almacenamiento en caché de objetos de Internet

No todos los objetos disponibles en la red son estáticos. Hay muchas páginas CGI generadas de forma dinámica, contadores de visitantes y documentos con contenido cifrado mediante SSL. Estos tipos de objetos no se almacenan en caché, dado que cambian cada vez que se accede a ellos.

La cuestión es cuánto tiempo deben permanecer en caché los demás objetos almacenados. Para determinarlo, a todos los objetos en caché se les asigna uno de los distintos estados posibles. Los servidores Web y alternos averiguan el estado de los objetos añadiéndoles encabezados como “Última modificación” o “Caduca”, junto a la fecha correspondiente. Otros encabezados especifican que los objetos no deben almacenarse en caché.

Los objetos en caché suelen sustituirse debido a la falta de espacio disponible en disco. Para ello se emplean algoritmos como el de uso más reciente (LRU). Básicamente, esto significa que el alterno desecha los objetos que no se han solicitado desde hace más tiempo.

29.2 Requisitos del sistema

Lo más importante es determinar la carga máxima de red que deberá soportar el sistema. Por lo tanto, es importante prestar más atención a los picos de carga, dado que pueden ser más de cuatro veces superiores a la media del día. Si tiene dudas, es preferible sobrestimar los requisitos del sistema, dado que si Squid funciona cerca de su límite de capacidad, puede provocar una pérdida importante de calidad del servicio. En las siguientes secciones se señalan los factores del sistema por orden de importancia.

29.2.1 Discos duros

La velocidad juega un papel importante en el proceso de almacenamiento en caché, por lo que este factor merece una atención especial. En el caso de los discos duros, este parámetro se describe como *tiempo de búsqueda aleatoria* y se mide en milésimas de segundo. Dado que los bloques de datos que Squid lee o escribe en el disco duro tienden a ser bastante pequeños, el tiempo de búsqueda del disco duro es más importante que la capacidad para proporcionar datos. Para los fines de un alterno, los discos duros con velocidades de rotación elevadas son probablemente la mejor elección, dado que permiten que el cabezal de lectura-escritura se coloque en el punto necesario más rápidamente. Una posibilidad para acelerar el sistema es utilizar varios discos al mismo tiempo o emplear matrices RAID.

29.2.2 Tamaño de caché de disco

En un caché pequeño, la probabilidad de una respuesta HIT (cuando se encuentra el objeto solicitado almacenado en caché) es pequeña, dado que el caché se llena fácilmente y los objetos menos solicitados se sustituyen con objetos más recientes. Por ejemplo, si hay un GB disponible para el almacenamiento en caché y los usuarios sólo descargan unos diez MB diarios al navegar, tardarán más de cien días en llenar el caché.

El modo más sencillo de determinar el tamaño de caché necesario es tener en cuenta la velocidad máxima de transferencia de la conexión. Con una conexión de 1 Mb/s, la velocidad máxima de transferencia es de 125 KB/s. Si todo este tráfico acaba en el caché, en una hora pueden llegar a añadirse hasta 450 MB y, suponiendo que sólo se genere tráfico en las ocho horas laborables, el total puede llegar a ser de hasta 3,6 GB por día. Dado que la conexión no suele utilizarse hasta el límite de su capacidad, puede suponerse que el volumen total de datos gestionados por el caché será de aproximadamente 2 GB. En nuestro ejemplo, se necesitarían 2 GB de espacio en disco para que Squid conserve en caché los datos de navegación de un día.

29.2.3 RAM

La cantidad de memoria (RAM) que Squid necesita es directamente proporcional al número de objetos almacenados en caché. Squid también almacena en la memoria principal referencias a los objetos en caché y los objetos solicitados con mayor frecuencia, a fin de acelerar la recuperación de estos datos. La memoria de acceso aleatorio es mucho más rápida que los discos duros.

Además, existen otros datos que Squid debe almacenar en la memoria, como una tabla con todas las direcciones IP gestionadas, un caché exacto de nombres de dominio, los objetos solicitados con mayor frecuencia, listas de control de acceso, buffers y otros elementos.

Es muy importante disponer de memoria suficiente para el proceso Squid, dado que el rendimiento del sistema sufre una reducción drástica si es necesario utilizar la memoria de intercambio del disco. La herramienta cachemgr.cgi puede utilizarse para la gestión de la memoria caché. Esta herramienta se presenta en la Sección 29.6, “cachemgr.cgi” (p. 575). Los sitios con un tráfico de red muy intenso deben tener en cuenta la posibilidad de utilizar sistemas AMD64 o Intel EM64T con más de 4 GB de memoria.

29.2.4 CPU

Squid no requiere un uso intensivo de la CPU. La carga del procesador sólo aumenta cuando se carga o comprueba el contenido del caché. El uso de un equipo con varios procesadores no aumenta el rendimiento del sistema. Para aumentar la eficacia, es preferible comprar discos más rápidos o añadir más memoria.

29.3 Inicio de Squid

Squid está ya preconfigurado en SUSE Linux. Puede empezar a utilizarse en cuanto concluye la instalación. Para garantizar un inicio fluido, debe configurar la red de modo que sea posible acceder al menos a Internet y a un servidor de nombres. Pueden surgir problemas si se emplea una conexión de acceso telefónico con una configuración de DNS dinámica. En este caso, debe introducir al menos el servidor de nombres, dado que Squid no se inicia si no detecta un servidor DNS en `/etc/resolv.conf`.

29.3.1 Comandos para iniciar y detener Squid

Para iniciar Squid, introduzca `rcsquid start` en la línea de comandos como usuario `Root`. Durante el primer inicio, deberá definir primero la estructura de directorios del caché en `/var/cache/squid`. El guión de inicio `/etc/init.d/squid` lleva a cabo automáticamente esta acción, que puede tardar unos pocos segundos o incluso minutos. Si a la derecha aparece `done` (Finalizado) en verde, Squid se ha cargado correctamente. Para probar la funcionalidad de Squid en el sistema local, introduzca `localhost` como alterno (proxy) y `3128` como puerto en el navegador.

Para permitir que usuarios del sistema local y de otros sistemas puedan acceder a Squid y a Internet, modifique la entrada del archivo de configuración `/etc/squid/squid.conf` de `http_access deny all` a `http_access allow all`. No obstante, tenga en cuenta que si lo hace, cualquier usuario podrá acceder sin restricciones a Squid. Por lo tanto, deberá definir listas ACL que controlen el acceso al alterno. Hay más información disponible acerca de este aspecto en la Sección 29.4.2, “Opciones de control de acceso” (p. 569).

Después de modificar el archivo de configuración `/etc/squid/squid.conf`, Squid deberá volver a cargarlo. Para ello, emplee el comando `rcsquid reload`. Si lo prefiere, utilice el comando `rcsquid restart` para reiniciar Squid completamente.

Puede emplear el comando `rcsquid status` para comprobar si el alterno se está ejecutando. El comando `rcsquid stop` detiene el funcionamiento de Squid. Esto puede tardar, dado que Squid espera hasta medio minuto (opción `shutdown_lifetime` en `/etc/squid/squid.conf`) antes de abandonar las conexiones de los clientes y escribir los datos en el disco.

AVISO: Cierre de Squid

El cierre de Squid con los comandos `kill` o `killall` puede dañar el caché. Para que sea posible reiniciar Squid, deberá suprimir el caché dañado.

Si Squid falla cuando transcurre un breve periodo de tiempo, aunque se haya iniciado correctamente, compruebe si hay una entrada de servidor de nombres errónea o si falta el archivo `/etc/resolv.conf`. Squid almacena los motivos de los errores de inicio en el archivo `/var/log/squid/cache.log`. Si Squid debe cargarse automáticamente al arrancar el sistema, utilice el editor de niveles de ejecución de YaST para activar Squid en los niveles de ejecución deseados. Consulte la Sección “Servicios de sistema (nivel de ejecución)” (Capítulo 2, *Configuración del sistema con YaST*, ↑Inicio).

Al desinstalar Squid no se elimina la jerarquía de caché ni los archivos de registro. Para eliminarlos, suprima el directorio `/var/cache/squid` manualmente.

29.3.2 Servidor DNS local

La configuración de un servidor DNS local puede resultar útil incluso aunque no gestione su propio dominio. En tal caso, actúa simplemente como un caché de servidor de nombres, y puede resolver solicitudes DNS mediante los servidores de nombres raíces sin que sea necesaria ninguna configuración especial (consulte la Sección 20.3, “Inicio del servidor de nombres BIND” (p. 406)). El modo en que se puede realizar esta acción depende de si se selecciona el ajuste de servicio de DNS dinámico durante la configuración de la conexión a Internet.

Servicio de DNS dinámico
: Si se selecciona el servicio de DNS dinámico, normalmente el proveedor de acceso define el servidor DNS al establecer la conexión a Internet, y el archivo local `/etc/resolv.conf` se ajusta automáticamente. Este comportamiento se controla mediante el archivo `/etc/sysconfig/network/config`, con la variable de configuración del sistema (sysconfig) `MODIFY_RESOLV_CONF_DYNAMICALLY`, que tiene el valor `"yes"` (Sí). Establezca el valor `"no"` para esta variable con el editor de configuración del sistema de YaST (consulte la Sección 8.3.1, “Cambio de la configuración del sistema mediante el editor YaST sysconfig” (p. 207)). A continuación, introduzca el servidor DNS local en el archivo `/etc/resolv.conf` con la dirección IP `127.0.0.1` para `localhost`. De este modo, Squid siempre encontrará el servidor de nombres local al iniciarse.

Para que sea posible acceder al servidor de nombres del proveedor, introdúzcalo junto a su dirección IP en la sección `forwarders` del archivo de configuración `/etc/named.conf`. Con el servicio DNS dinámico, puede hacer que este paso se lleve a cabo automáticamente al establecer la conexión, definiendo el valor `YES` (Sí) en la variable de configuración del sistema (sysconfig) `MODIFY_NAMED_CONF_DYNAMICALLY`.

Servicio DNS estático
: Con el servicio DNS estático, no se lleva a cabo ningún ajuste automático de DNS al establecer la conexión, por lo que no es necesario modificar ninguna variable de configuración del sistema. No obstante, deberá introducir el servidor DNS local en el archivo `/etc/resolv.conf`, tal y como se ha descrito anteriormente. Además, también deberá introducir manualmente el servidor de nombres estático del proveedor y su dirección IP en la sección `forwarders` del archivo `/etc/named.conf`.

SUGERENCIA: DNS y cortafuegos

Si utiliza un cortafuegos, compruebe que las solicitudes DNS pueden atravesarlo.

29.4 Archivo de configuración /etc/squid/squid.conf

Todos los ajustes del servidor alterno Squid se realizan en el archivo `/etc/squid/squid.conf`. Para iniciar Squid por primera vez, no es necesario realizar ningún cambio en este archivo, pero al principio se deniega el acceso a los clientes externos. El alterno sólo está disponible para `localhost`. El puerto por defecto es el `3128`. El archivo de configuración preinstalado, `/etc/squid/squid.conf`, proporciona información detallada sobre las opciones y muchos ejemplos. Casi todas las entradas empiezan por # (las líneas tienen comentarios) y las especificaciones relevantes se encuentran al final de las líneas. Los valores dados normalmente se corresponden con los valores por defecto, por lo que eliminar los signos de comentarios sin cambiar los parámetros suele producir pocos cambios en la mayoría de los casos. Si es posible, no modifique los ejemplos e introduzca las opciones junto a los parámetros modificados en la línea siguiente. De este modo, podrá recuperar fácilmente los valores por defecto y compararlos con los cambios en cualquier momento.

SUGERENCIA: Adaptación del archivo de configuración después de una actualización

Si ha efectuado una actualización a partir de una versión anterior de Squid, es recomendable editar el nuevo archivo `/etc/squid/squid.conf` y aplicar sólo los cambios realizados en el archivo anterior. Si intenta utilizar el archivo `squid.conf` anterior, es posible que la configuración ya no funcione, dado que a veces se modifican las opciones y se añaden nuevos cambios.

29.4.1 Opciones de configuración generales (selección)

http_port 3128
: Este es el puerto que Squid utiliza para escuchar las solicitudes de los clientes. El puerto por defecto es el `3128`, pero el `8080` también suele utilizarse. Si lo desea, puede especificar varios números de puerto separados por espacios.

cache_peer *`nombre de host`* *`tipo`* *`puerto del alterno`* *`puerto icp`*
: Introduzca un alterno principal, por ejemplo, si desea utilizar el alterno del proveedor de Internet. Como *`nombre de host`*, introduzca el nombre y la dirección IP del alterno que desee utilizar y como *`tipo`*, introduzca `parent`. En *`puerto del alterno`*, introduzca el número de puerto proporcionado por el operador del alterno principal para su uso en el navegador, normalmente será el `8080`. Establezca los valores `7` o `0` para el *`puerto icp`* si el puerto ICP del alterno principal es desconocido y su uso es irrelevante para el proveedor. También puede especificar `default` y `no-query` tras los números de puerto para impedir el uso del protocolo ICP. En tal caso, Squid se comportará como un navegador normal por lo que al alterno del proveedor respecta.

cache_mem 8 MB
: Esta entrada define la cantidad de memoria que puede emplear Squid para las respuestas más frecuentes. El valor por defecto es `8 MB`. Este valor no especifica el uso total de memoria de Squid, por lo que es posible que el uso real sea superior.

cache_dir ufs /var/cache/squid/ 100 16 256
: La entrada *cache_dir* define el directorio del disco en el que se almacenan todos los objetos. Los números del final indican el espacio máximo en disco que debe utilizarse en MB y el número de directorios de primer y segundo nivel. El parámetro

`ufs` no debe modificarse. Los valores por defecto implican 100 MB de espacio ocupado en disco por el directorio `/var/cache/squid` y la creación de 16 subdirectorios en él, cada uno de los cuales contiene 256 subdirectorios adicionales. Al especificar el espacio en disco que desea utilizar, reserve espacio suficiente. Los valores más adecuados oscilan entre un mínimo del 50% y un máximo del 80% del espacio disponible en disco. Debe extremar las precauciones si decide aumentar los dos últimos números (referentes a los directorios), dado que la existencia de demasiados directorios puede provocar problemas de rendimiento. Si tiene varios discos que comparten el caché, introduzca varias líneas *cache_dir*.

cache_access_log /var/log/squid/access.log, cache_log /var/log/squid/cache.log, cache_store_log /var/log/squid/store.log
: Estas tres entradas especifican las rutas en las que Squid registra todas sus acciones. Normalmente no es necesario realizar ningún cambio. Si Squid experimenta una carga de uso intensa, puede que resulte útil distribuir el caché y los archivos de registro en varios discos.

emulate_httpd_log off
: Si la entrada tiene el valor *on,* obtendrá archivos de registro legibles. No obstante, algunos programas de evaluación no podrán interpretarlos.

client_netmask 255.255.255.255
: Esta entrada permite enmascarar las direcciones IP de los clientes en los archivos de registro. El último dígito de la dirección IP tendrá el valor cero si introduce aquí `255.255.255.0`. De ese modo, puede proteger la privacidad de los clientes.

ftp_user Squid@
: Permite definir la contraseña que debe utilizar Squid para los inicios de sesión FTP anónimos. Puede que sea una buena idea indicar una dirección de correo electrónico válida, dado que algunos servidores FTP las comprueban para verificar su validez.

cache_mgr webmaster
: Una dirección de correo electrónico a la que Squid debe enviar un mensaje si se produce un error inesperado. El valor por defecto es *webmaster.*

logfile_rotate 0
: Si ejecuta `squid -k rotate`, `Squid` puede rotar los archivos de registro protegidos. Los archivos se numeran durante el proceso y, al llegar al valor especificado, se sobrescribe el archivo más antiguo. El valor por defecto es `0`, dado que el almacenamiento y la supresión de archivos de registro en SUSE Linux se

lleva a cabo mediante un cronjob establecido en el archivo de configuración `/etc/logrotate/squid`.

append_domain <dominio>
: Utilice *append_domain* para especificar el dominio que debe adjuntarse automáticamente si no se proporciona ninguno. Normalmente se introduce su propio dominio, por lo que al introducir *www* en el navegador accederá a su propio servidor Web.

forwarded_for on
: Si establece el valor *off* para esta entrada, Squid eliminará la dirección IP y el nombre de sistema de los clientes de las solicitudes HTTP. De lo contrario, añadirá al encabezado una línea similar a la siguiente:

```
X-Forwarded-For: 192.168.0.0
```

negative_ttl 5 minutes; negative_dns_ttl 5 minutes
: Por lo general, no necesita efectuar ningún cambio en estos valores. No obstante, si utiliza una conexión de acceso telefónico, en ocasiones puede que no sea posible acceder a Internet. Squid tiene en cuenta las solicitudes fallidas y rechaza emitir solicitudes nuevas, aunque la conexión a Internet se restablezca. Si esto ocurre, cambie el valor de *minutes* (minutos) a *seconds* (segundos) y haga clic en el botón de *actualización* del navegador, el proceso de marcación debería volver a iniciarse en unos segundos.

never_direct allow *`nombre_acl`*
: Para evitar que Squid acepte solicitudes directamente de Internet, utilice el comando anterior para forzar la conexión con otro alterno. Dicho alterno deberá haberse introducido anteriormente en *cache_peer*. Si especifica el valor `all` para la entrada *`acl_name`*, forzará todas las solicitudes de modo que se envíen directamente al alterno *principal*. Esto puede resultar necesario, por ejemplo, si emplea un proveedor que estipula de forma estricta el uso de sus alternos o deniega al cortafuegos acceso directo a Internet.

29.4.2 Opciones de control de acceso

Squid proporciona un sistema detallado para controlar el acceso al alterno. La configuración de dicho sistema es muy sencilla y completa mediante la implementación de ACL. Esto implica listas con reglas que se procesan de forma secuencial. Las listas ACL deben definirse antes de proceder a su uso. Algunas listas ACL, como *all* y

localhost, ya existen. No obstante, la definición de una lista ACL no implica automáticamente su aplicación. Esto sólo ocurre con las reglas *http_access*.

acl <nombre_acl> <tipo> <datos>
: Una lista ACL requiere al menos tres especificaciones para su definición. El nombre *<nombre_acl>* puede elegirse arbitrariamente. En *<tipo>,* seleccione entre la variedad de opciones diferentes que encontrará en la sección *ACCESS CONTROLS* (Controles de acceso) del archivo `/etc/squid/squid.conf`. La especificación de *<datos>* depende del tipo de ACL individual y también puede leerse desde un archivo, por ejemplo mediante nombres de hosts, direcciones IP o direcciones URL. A continuación encontrará algunos ejemplos sencillos:

```
acl misusuarios srcdomain .midominio.com
acl profesores src 192.168.1.0/255.255.255.0
acl alumnos src 192.168.7.0-192.168.9.0/255.255.255.0
acl hora del almuerzo MTWHF 12:00-15:00
```

http_access allow <nombre_acl>
: *http_access* define quién puede utilizar el alterno y quién puede acceder a qué en Internet. Para que esto sea posible, deberá proporcionar listas ACL. *localhost* y *all* ya se han definido anteriormente y pueden permitir o denegar el acceso mediante los valores *deny* (Denegar) y *allow* (Permitir). Puede crear una lista con cualquier número de entradas *http_access*, que se procesarán de arriba a abajo y, dependiendo de lo que ocurra primero, permitirán o denegarán el acceso a la dirección URL respectiva. La última entrada siempre debe ser *http_access deny all*. En el siguiente ejemplo *localhost* (host local) tiene acceso a todo, mientras que a todos los demás hosts se les deniega el acceso completamente.

```
http_access allow localhost
http_access deny all
```

En otro ejemplo de uso de estas reglas, el grupo `profesores` siempre tiene acceso a Internet. El grupo `alumnos` sólo tiene acceso de lunes a viernes durante la hora del almuerzo.

```
http_access deny localhost
http_access allow profesores
http_access allow alumnos hora del almuerzo
http_access deny all
```

En beneficio de la legibilidad del archivo, la lista con las entradas *http_access* sólo debe introducirse en la posición designada en el archivo `/etc/squid/squid.conf`. Es decir, entre el texto

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
# CLIENTS
```

y la última entrada

```
http_access deny all
```

redirect_program /usr/bin/squidGuard
: Esta opción permite especificar un redireccionador como squidGuard, que permite bloquear las direcciones URL no deseadas. El acceso a Internet se puede controlar de forma individualizada para distintos grupos de usuarios mediante la autenticación de alternos y las listas ACL adecuadas. squidGuard es un paquete aparte que puede instalarse y configurarse por separado.

auth_param basic program /usr/sbin/pam_auth
: Si los usuarios deben autenticarse en el alterno, defina un programa adecuado, como pam_auth. Al acceder a pam_auth por primera vez, el usuario verá una ventana de inicio de sesión en la que podrá introducir el nombre de usuario y la contraseña. Además, sigue siendo necesaria una lista ACL, por lo que sólo los clientes con un inicio de sesión válido podrán utilizar Internet:

```
acl password proxy_auth REQUIRED

http_access allow password
http_access deny all
```

El valor *REQUIRED* tras *proxy_auth* puede sustituirse con una lista de nombres de usuario permitidos o con la vía a dicha lista.

ident_lookup_access allow <nombre_acl>
: Permite ejecutar una solicitud de identidad para todos los clientes definidos en la lista ACL para averiguar la identidad de cada usuario. Si incluye *all* en *<nombre_acl>*, la solicitud será válida para todos los clientes. Además, deberá haber un daemon de identidad en ejecución en todos los clientes. En Linux, instale el paquete pidentd. En el caso de Microsoft Windows, en Internet encontrará software gratuito disponible para su descarga. Para garantizar que sólo se permitan los clientes con una búsqueda de identidad correcta, defina la lista ACL correspondiente aquí:

```
acl identhosts ident REQUIRED

http_access allow identhosts
http_access deny all
```

En esta entrada también puede sustituir *REQUIRED* por una lista de nombres de usuario permitidos. El uso de *ident* puede ralentizar bastante el tiempo de acceso, dado que las búsquedas de identidad se repiten para cada solicitud.

29.5 Configuración de un alterno transparente

El método habitual de trabajo con los servidores alternos es el siguiente: el navegador Web envía solicitudes a un puerto concreto del servidor alterno y éste proporciona los objetos solicitados, estén o no almacenados en caché. Al trabajar en red, pueden darse varias situaciones:

- Por motivos de seguridad, es recomendable que todos los clientes utilicen un alterno para navegar por Internet.
- Todos los clientes deben utilizar un alterno, sean conscientes de ello o no.
- El alterno de una red cambia de ubicación, pero los clientes existentes deben conservar la configuración antigua.

En todos estos casos, puede utilizarse un alterno transparente. El principio es muy sencillo: el alterno intercepta y responde a las solicitudes del navegador Web, por lo que el navegador Web recibe las páginas solicitadas sin saber de dónde proceden. Como su propio nombre indica, todo el proceso se lleva a cabo de forma transparente.

29.5.1 Opciones de configuración de /etc/squid/squid.conf

Las opciones que debe activar en el archivo `/etc/squid/squid.conf` para que el alterno transparente funcione correctamente son las siguientes:

- `httpd_accel_host` virtual
- `httpd_accel_port` 80

  Número de puerto donde se encuentra el servidor HTTP real

- `httpd_accel_with_proxy` on
- `httpd_accel_uses_host_header` on

29.5.2 Configuración de cortafuegos con SuSEfirewall2

Ahora se redireccionarán todas las solicitudes entrantes mediante el cortafuegos, con la ayuda de una regla de reenvío de puertos orientada al puerto de Squid. Para ello, utilice la herramienta SuSEfirewall2 incluida, descrita en la “Configuración con YaST” (p. 116). Su archivo de configuración se encuentra en `/etc/sysconfig/SuSEfirewall2`. El archivo de configuración está compuesto por entradas bien documentadas. Para establecer un alterno transparente, deberá configurar varias opciones del cortafuegos:

- Dispositivo dirigido a Internet: `FW_DEV_EXT`="eth1"
- Dispositivo dirigido a la red: `FW_DEV_INT`="eth0"

Defina en el cortafuegos los puertos y servicios (consulte `/etc/services`) a los que se debe acceder desde las redes no fiables (externas) como Internet. En este ejemplo, sólo se ofrecen al exterior servicios Web:

```
FW_SERVICES_EXT_TCP="www"
```

Defina en el cortafuegos los puertos o servicios (consulte `/etc/services`) a los que se debe acceder desde la red segura (interna), mediante TCP y UDP:

```
FW_SERVICES_INT_TCP="domain www 3128"
FW_SERVICES_INT_UDP="domain"
```

En este ejemplo, se permite el acceso a los servicios Web y a Squid (cuyo puerto por defecto es el `3128`). El servicio “domain” significa DNS (servicio de nombres de dominio). Este servicio se utiliza muy frecuentemente. Si no es así, basta con borrar las entradas anteriores y establecer el valor `no` en la siguiente opción:

```
FW_SERVICE_DNS="yes"
```

La opción más importante es la número `15:`

Ejemplo 29.1 *Configuración de cortafuegos: opción 15*

```
# 15.)
# Which accesses to services should be redirected to a local port
# on the firewall machine?
#
# This can be used to force all internal users to surf via your
# Squid proxy, or transparently redirect incoming Web traffic to
# a secure Web server.
#
# Choice: leave empty or use the following explained syntax of
# redirecting rules, separated with spaces.
# A redirecting rule consists of 1) source IP/net,
# 2) destination IP/net, 3) original destination port and
# 4) local port to redirect the traffic to, separated by a colon,
# e.g. "10.0.0.0/8,0/0,80,3128 0/0,172.20.1.1,80,8080"
```

Los comentarios anteriores muestran la sintaxis que debe seguirse. En primer lugar, introduzca la dirección IP y la máscara de red de las redes internas que acceden al cortafuegos del alterno. En segundo lugar, introduzca la dirección IP y la máscara de red a las que los clientes envían las solicitudes. En el caso de los navegadores Web, especifique las redes `0/0`, un comodín que significa "a todas partes". Después de eso, introduzca el puerto original al que se envían las solicitudes y, finalmente, el puerto al que se redireccionan todas las solicitudes. Dado que Squid es compatible con otros protocolos además de HTTP, redirija al alterno las solicitudes de otros puertos, como FTP (puerto 21), HTTPS o SSL (puerto 443). En este ejemplo, los servicios Web (puerto `80`) se redireccionan al puerto del alterno (puerto `3128`). Si hay más redes o servicios que añadir, deben separarse mediante un espacio en blanco en la entrada respectiva.

```
FW_REDIRECT_TCP="192.168.0.0/16,0/0,80,3128 192.168.0.0/16,0/0,21,3128"
FW_REDIRECT_UDP="192.168.0.0/16,0/0,80,3128 192.168.0.0/16,0/0,21,3128"
```

Para iniciar el cortafuegos y la nueva configuración, modifique una entrada del archivo `/etc/sysconfig/SuSEfirewall2`. La entrada `START_FW` debe tener el valor `"yes"` (Sí).

Inicie Squid tal y como se describe en la Sección 29.3, "Inicio de Squid" (p. 564). Para comprobar si todo funciona correctamente, acceda a los registros de Squid en `/var/log/squid/access.log`. Para comprobar que todos los puertos están configurados correctamente, lleve a cabo una exploración de puertos en el equipo desde cualquier equipo que esté fuera de la red. Sólo debe estar abierto el puerto de los servicios Web (el 80). Para explorar los puertos con nmap, la sintaxis del comando es `nmap -O dirección_IP`.

29.6 cachemgr.cgi

El gestor de caché (cachemgr.cgi) es una utilidad CGI que muestra estadísticas sobre el uso de memoria de los procesos Squid en ejecución. También es un modo más cómodo de gestionar el caché y ver las estadísticas sin generar registros en el servidor.

29.6.1 Instalación

En primer lugar, es necesario que exista un servidor Web en ejecución en el sistema. Configure Apache tal y como se describe en el Capítulo 26, *Servidor HTTP Apache* (p. 483). Para comprobar si Apache ya se está ejecutando, introduzca el comando `rcapache status` como usuario `Root`. Si aparece un mensaje similar al siguiente:

```
Checking for service httpd: OK
Server uptime: 1 day 18 hours 29 minutes 39 seconds
```

Apache se está ejecutando en el equipo. Si no es así, introduzca `rcapache start` para iniciar Apache con los ajustes por defecto para SUSE Linux. El último paso para configurarlo es copiar el archivo `cachemgr.cgi` en el directorio `cgi-bin` de Apache:

```
cp /usr/share/doc/packages/squid/scripts/cachemgr.cgi /srv/www/cgi-bin/
```

29.6.2 Listas ACL del gestor de caché en /etc/squid/squid.conf

Algunos ajustes por defecto del archivo original son necesarios para el gestor de caché. En primer lugar, se definen dos listas ACL, a continuación, las opciones http_access utilizan dichas listas para proporcionar acceso a Squid al guión CGI. La primera lista ACL es la más importante, dado que el gestor de caché intenta comunicarse con Squid mediante el protocolo cache_object.

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
```

Las siguientes reglas proporcionan a Apache los derechos de acceso a Squid:

```
http_access allow manager localhost
http_access deny manager
```

Estas reglas presuponen que el servidor Web y Squid se ejecutan en el mismo equipo. Si la comunicación entre el gestor de caché y Squid se origina en un servidor Web de otro equipo, incluya una lista ACL adicional, como en el Ejemplo 29.2, “Reglas de acceso” (p. 576).

Ejemplo 29.2 *Reglas de acceso*

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl webserver src 192.168.1.7/255.255.255.255 # webserver IP
```

A continuación, añada las reglas del Ejemplo 29.3, “Reglas de acceso” (p. 576) para permitir el acceso desde el servidor Web.

Ejemplo 29.3 *Reglas de acceso*

```
http_access allow manager localhost
http_access allow manager webserver
http_access deny manager
```

Configure una contraseña para el gestor a fin de proporcionarle acceso a más opciones, como el cierre remoto del caché o la visualización de información de caché adicional. Para ello, configure la entrada `cachemgr_passwd` con una contraseña para el gestor y la lista de opciones. Esta lista aparecerá como parte de los comentarios de la entrada en `/etc/squid/squid.conf`.

Reinicie Squid siempre que modifique el archivo de configuración. Para ello, emplee el comando `rcsquid reload`.

29.6.3 Visualización de las estadísticas

Visite el sitio Web correspondiente: `http://webserver.example.org/cgi-bin/cachemgr.cgi`. Haga clic en *Continue* (Continuar) y desplácese por las diferentes estadísticas. Encontrará más información sobre cada una de las entradas que muestra el gestor de caché en las preguntas frecuentes sobre Squid, en la siguiente dirección: `http://www.squid-cache.org/Doc/FAQ/FAQ-9.html`.

29.7 squidGuard

El objetivo de esta sección no es detallar cómo es una configuración exhaustiva de squidGuard, sino únicamente presentar la aplicación y proporcionar algunos consejos para utilizarla. Para obtener información más detallada sobre la configuración, consulte el sitio Web de squidGuard en la siguiente dirección: `http://www.squidguard.org`.

squidGuard es un complemento de licencia libre (GPL) para Squid que funciona como filtro, redireccionador y controlador de acceso flexible y rápido. Permite definir varias reglas de acceso con diferentes restricciones para diferentes grupos de usuarios de un caché de Squid. La utilidad squidGuard utiliza la interfaz de redirección estándar de Squid y permite hacer lo siguiente:

- Limitar el acceso Web para algunos usuarios a una lista de servidores Web o direcciones URL aceptados o conocidos.
- Bloquear el acceso a algunos servidores Web o direcciones URL de una lista para algunos usuarios.
- Bloquear el acceso a las direcciones URL que coincidan con una lista de expresiones regulares o palabras para algunos usuarios.
- Redirigir las direcciones URL a una página de información “inteligente” basada en CGI.
- Redirigir a los usuarios no registrados a un formulario de registro.
- Redirigir los anuncios a un archivo GIF vacío.
- Utilizar diferentes reglas de acceso basadas en la hora del día, el día de la semana, la fecha, etc.
- Utilizar reglas diferentes para distintos grupos de usuarios.

Squid y squidGuard no pueden utilizarse para:

- Editar, filtrar o censurar el texto que contienen los documentos.
- Editar, filtrar o censurar los lenguajes de guiones incrustados en archivos HTML, como JavaScript o VBscript.

Antes de utilizarlo, instale `squidGuard`. Proporcione un archivo de configuración mínima, como `/etc/squidguard.conf`. Encontrará ejemplos de configuración en `http://www.squidguard.org/config/`. Más adelante, podrá experimentar con ajustes de configuración más complicados.

A continuación, cree una página falsa de "acceso denegado" o una página CGI relativamente compleja para redirigir a Squid si el cliente solicita un sitio Web incluido en una lista negra. Se recomienda encarecidamente el uso de Apache.

Ahora, configure Squid para utilizar squidGuard. Utilice la siguiente entrada del archivo `/etc/squid/squid.conf`:

```
redirect_program /usr/bin/squidGuard
```

Otra opción, denominada `redirect_children`, permite configurar el número de procesos de "redirección" (en este caso de squidGuard) que se deben ejecutar en el equipo. squidGuard es lo suficientemente rápido para gestionar muchas solicitudes: en un equipo Pentium a 500 MHz con 5.900 dominios y 7.880 direcciones URL (lo que suma un total de 13.780), puede procesar 100.000 solicitudes en 10 segundos. Por lo tanto, no es recomendable configurar más de cuatro procesos, dado que la asignación de estos procesos consumiría una cantidad excesiva de memoria.

```
redirect_children 4
```

Por último, haga que Squid cargue la nueva configuración ejecutando el comando `rcsquid reload`. Ahora, pruebe los ajustes con un navegador.

29.8 Generación de informes de caché con Calamaris

Calamaris es un guión de Perl utilizado para generar informes de la actividad de caché en formato ASCII o HTML. Es compatible con los archivos de registro de acceso nativos de Squid. La página de Calamaris se encuentra en la siguiente dirección: `http://Calamaris.Cord.de/`. El programa es muy sencillo de utilizar.

Inicie sesión como usuario `Root` e introduzca `cat access.log.files | calamaris` *`opciones`* `> archivodeinforme`. Al conducir varios archivos de registro es importante que estén ordenados cronológicamente, de mayor a menor antigüedad. A continuación describiremos algunas opciones del programa:

-a
: Muestra todos los informes disponibles.

-w
: Muestra los informes en formato HTML.

-l
: Incluye un mensaje o logotipo en el encabezado del informe.

En la página Man del programa encontrará más información sobre las distintas opciones. Para consultarla, utilice el comando `man calamaris`.

Un ejemplo habitual de uso es el siguiente:

```
cat access.log.2 access.log.1 access.log | calamaris -a -w \
> /usr/local/httpd/htdocs/Squid/informedesquid.html
```

Este comando coloca el informe en el directorio del servidor Web. Se necesita la aplicación Apache para ver los informes.

Otra potente herramienta de generación de informes de caché es SARG (Squid Analysis Report Generator, generador de informes de análisis de Squid). Encontrará más información sobre esta herramienta en la siguiente dirección: `http://sarg.sourceforge.net/`.

29.9 Información adicional

Visite la página de Squid en la siguiente dirección: `http://www.squid-cache.org/`. En ella encontrará el documento “Squid User Guide” (Guía del usuario de Squid) y una extensa recopilación de las preguntas más frecuentes sobre Squid.

Una vez realizada la instalación, encontrará una pequeña guía de procedimientos sobre los alternos transparentes en `howtoenh`, dentro de `/usr/share/doc/howto/en/txt/TransparentProxy.gz`. También tiene a su disposición las listas de correo sobre Squid en la siguiente dirección: `squid-users@squid-cache.org`. El archivo de reserva de la lista de correo se encuentra en `http://www.squid-cache.org/mail-archive/squid-users/`.

Parte 5. Movilidad

30 Informática móvil con Linux

La informática móvil se asocia comúnmente a los equipos portátiles, los dispositivos PDA y los teléfonos móviles, y al intercambio de datos entre ellos. Los componentes de hardware móviles como, por ejemplo, los discos duros externos, las unidades flash o las cámaras digitales pueden conectarse a portátiles y a sistemas de escritorio. Hay un buen número de componentes de software que están adaptados a la informática móvil e, incluso, algunas aplicaciones están diseñadas específicamente para este uso.

30.1 Equipos portátiles

El hardware para equipos portátiles difiere del hardware para sistemas de escritorio normales. Esto se debe a que ciertos criterios, como la intercambiabilidad, el espacio ocupado y el consumo de energía son propiedades fundamentales. Los fabricantes de hardware móvil han desarrollado el estándar PCMCIA (Asociación internacional de tarjetas de memoria para computadoras personales). Este estándar cubre tarjetas de memoria, tarjetas de interfaz de red, tarjetas de módem y RDSI y discos duros externos. El Capítulo 31, *PCMCIA* (p. 595) describe la compatibilidad para este tipo de hardware en Linux, qué necesidades han de tenerse en cuenta a la hora de configurarlo, qué software hay disponible para controlar los componentes PCMCIA y cómo solucionar posibles problemas.

30.1.1 Conservación de energía

En la fabricación de equipos portátiles, la inclusión de componentes de sistema de consumo optimizado de energía contribuye a su idoneidad para usarse en caso de no

tener acceso a la red de suministro eléctrico. Su contribución con respecto a la conservación de energía es, cuanto menos, tan importante como el sistema operativo. SUSE Linux admite varios métodos que influyen en el consumo de energía de un equipo portátil y afectan de distinta manera al tiempo de funcionamiento con batería. La siguiente lista aparece en orden descendente en cuanto a contribución a conservación de la energía:

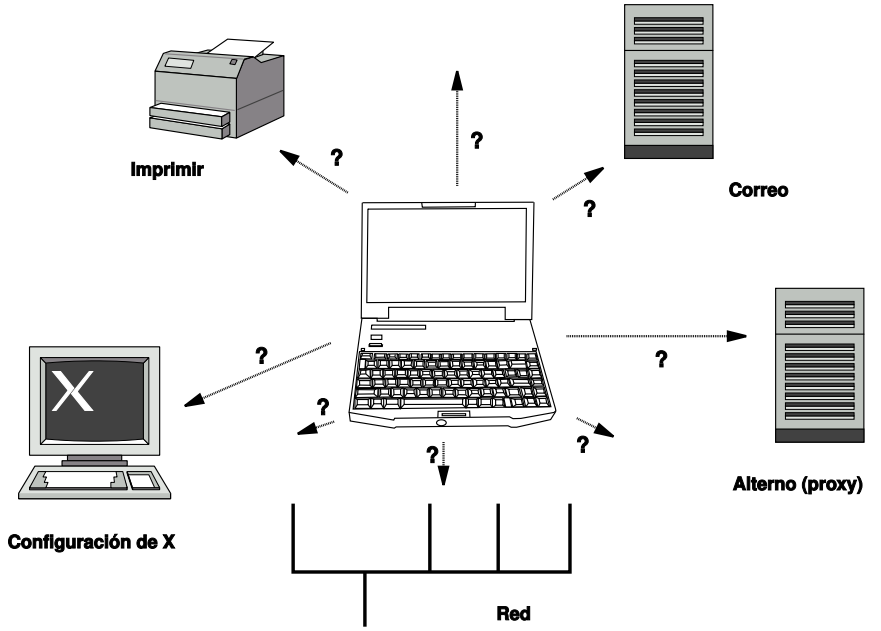
- Limitación de la velocidad de la CPU
- Desconexión de la iluminación de la pantalla en las pausas
- Ajuste manual de la iluminación de la pantalla
- Desconexión de accesorios HotPlug no utilizados (CD-ROM USB, ratón externo, tarjetas PCMCIA no utilizadas, etc.)
- Reducción de la rotación del disco duro en estado inactivo

Hay más información detallada sobre gestión de energía en SUSE Linux y sobre cómo utilizar el módulo de gestión de energía de YaST en el Capítulo 33, *Gestión de energía* (p. 621).

30.1.2 Integración en entornos operativos cambiantes

El sistema necesita adaptarse a los entornos operativos cambiantes si se le quiere dar un uso móvil. Muchos servicios dependen del entorno y deben volver a configurarse clientes subyacentes. SUSE Linux gestiona esta tarea en su lugar.

Figura 30.1 *Integración de equipos portátiles en redes*



Los servicios que se ven afectados cuando el equipo portátil cambia constantemente de una pequeña red casera a una red de oficina y viceversa son:

Red
: Este servicio incluye la asignación de dirección IP, resolución de nombres, conectividad a Internet y conectividad a otras redes.

Impresión
: Dependiendo de la red, es necesario disponer de una base de datos con impresoras disponibles y un servidor de impresión disponible.

Correo electrónico y alternos
: Al igual que para la impresión, la lista de servidores correspondientes debe estar actualizada.

X
: Si el equipo portátil está temporalmente conectado a un proyector o a un monitor externo, deberán estar disponibles las diferentes configuraciones de pantalla.

SUSE Linux ofrece varias maneras de integrar un equipo portátil en los entornos operativos existentes.

SCPM
: SCPM (gestión de perfiles de configuración de sistemas) permite almacenar estados de configuración arbitrarios de un sistema en una especie de "instantánea" que recibe el nombre de *perfil*. Los perfiles se pueden crear con vistas a situaciones diferentes y resultan útiles cuando el sistema trabaja en entornos cambiantes (redes domésticas y de oficina). Siempre se puede cambiar de un perfil a otro. Encontrará más información acerca de SCPM en el Capítulo 32, *Gestión de perfiles de la configuración del sistema* (p. 605). Podrá usar el applet de inicio Profile Chooser (Selector de perfiles) de KDE para cambiar de un perfil a otro. La aplicación exige la contraseña raíz antes de cambiar entre un perfil y otro.

NetworkManager
: NetworkManager está especialmente diseñado para la conectividad móvil en portátiles. Ofrece un medio para cambiar de forma sencilla y automática entre entornos de red o distintos tipos de redes, como LAN inalámbricas y Ethernet. NetworkManager es compatible con el cifrado WEP y WPA-PSK en redes LAN inalámbricas y en conexiones de acceso telefónico (con smpppd). Ambos entornos de escritorio (GNOME y KDE) incluyen una interfaz de usuario para NetworkManager.

Tabla 30.1 *Casos de utilización de NetworkManager*

Mi equipo…	**Usa NetworkManager**
es un portátil	Yes
está conectado a veces a redes distintas	Yes
ofrece servicios de red (como DNS o DHCP)	No
sólo usa una dirección IP estática	No

Utilice las herramientas de YaST para configurar la conectividad siempre que NetworkManager no deba gestionar la configuración de red.

SLP
: El protocolo de ubicación de servicios (SLP) simplifica la conexión de los portátiles a las redes existentes. Sin SLP, el administrador del portátil normalmente necesitaría un detallado conocimiento de los servicios disponibles en la red. SLP difunde la disponibilidad de ciertos tipos de servicios a todos los clientes de la red local. Las aplicaciones compatibles con SLP pueden procesar la información emitida por SLP y se pueden configurar automáticamente. SLP puede utilizarse incluso para instalar un sistema y evitar así la necesidad de buscar fuentes de instalación adecuadas. Hay más información detallada acerca de SLP en el Capítulo 19, *Servicios SLP en la red* (p. 393).

La importancia de SCPM recae en la posibilidad de habilitar y mantener condiciones de sistema reproducibles. SLP facilita en gran manera la tarea de configurar equipos en red automatizando gran parte del proceso.

30.1.3 Opciones de software

Hay varias tareas especiales en el uso móvil de las cuales se encargan programas de software dedicados: la monitorización del sistema (especialmente la carga de la batería), la sincronización de datos y la comunicación inalámbrica con periféricos e Internet. Las secciones siguientes tratan sobre las aplicaciones más importantes que utiliza SUSE Linux para cada tarea.

Monitorización del sistema

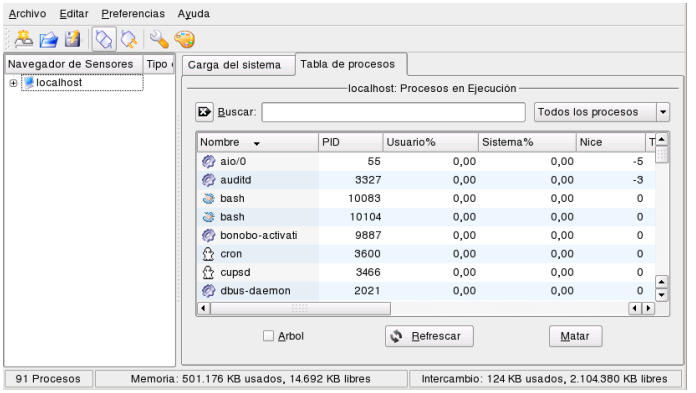
SUSE Linux incluye dos herramientas de monitorización del sistema de KDE.

KPowersave
: KPowersave es un applet que muestra el estado de la batería recargable en el panel de control. El icono se adapta al tipo de suministro eléctrico. Si se trabaja con suministro de CA, aparece el icono de un pequeño enchufe. Si se trabaja con baterías, el icono cambia a una batería. El menú correspondiente abre el módulo de YaST de gestión de energía después de solicitar la contraseña raíz. Esto permite definir el comportamiento del sistema bajo diferentes tipos de suministro de energía. Encontrará información sobre la gestión de energía y sobre el módulo de YaST correspondiente en el Capítulo 33, *Gestión de energía* (p. 621).

KSysguard

KSysguard es una aplicación independiente que reúne todos los parámetros medibles del sistema en un entorno de monitorización. KSysguard tiene monitores para ACPI (estado de la batería), carga de la CPU, red, particiones y uso de la memoria. También puede ver y mostrar todos los procesos del sistema. Es posible personalizar la presentación y el filtrado de los datos recopilados. Se pueden monitorizar diferentes parámetros del sistema en varias páginas de datos o recopilar los datos de varias máquinas en paralelo a través de la red. KSysguard también se puede ejecutar como un daemon en máquinas sin un entorno KDE. Encontrará más información sobre este programa en su función de ayuda integrada o en las páginas de ayuda de SUSE.

Figura 30.2 *Monitorización del estado de la batería con KSysguard*



En el escritorio de GNOME, use el applet de panel (GNOME ACPI) y el Monitor del sistema de las aplicaciones.

Sincronización de los datos

Cuando se pasa de trabajar en una máquina móvil desconectada de la red a trabajar en una estación de trabajo en red dentro de una oficina, es necesario mantener los datos procesados sincronizados en todas las instancias. Esto puede incluir carpetas de correo electrónico y de directorios y archivo individuales que deben estar presentes para trabajar tanto fuera como dentro de la oficina. La solución en ambos casos es la siguiente:

Sincronización del correo electrónico
: Utilice una cuenta IMAP para almacenar sus mensajes de correo electrónico en la red de la oficina. A continuación, acceda a los mensajes de correo electrónico desde la estación de trabajo mediante cualquier cliente de correo electrónico compatible con IMAP desconectado, como Mozilla Thunderbird Mail, Evolution o KMail, tal y como se describe en *Aplicaciones*. El cliente de correo electrónico debe estar configurado de modo que se entre siempre en la misma carpeta para los `mensajes enviados`. Esto garantiza que todos los mensajes estén disponibles, junto con la información de estado, después de terminar el proceso de sincronización. Utilice un servidor SMTP implementado en el cliente de correo para enviar mensajes en lugar de Postfix de MTA para todo el sistema o Sendmail para recibir información fiable acerca del correo no enviado.

Sincronización de archivos y directorios
: Hay varias utilidades disponibles para sincronizar datos entre un equipo portátil y una estación de trabajo. Para obtener información detallada, consulte el Capítulo 27, *Sincronización de archivos* (p. 525).

Comunicación inalámbrica

Al igual que pueden conectarse a la red doméstica o a la de la oficina con un cable, los equipos portátiles también pueden conectarse inalámbricamente a otros equipos, periféricos, teléfonos móviles o dispositivos PDA. Linux admite tres tipos de comunicación inalámbrica:

WLAN
: Con el mayor alcance dentro de las tecnologías inalámbricas, WLAN es la única tecnología adecuada para trabajar con redes amplias y a veces separadas en el espacio. Las máquinas se pueden conectar entre sí para formar una red inalámbrica independiente o para acceder a Internet. Unos dispositivos llamados "puntos de acceso" funcionan como estaciones base para los dispositivos con WLAN habilitado y actúan como intermediarios para acceder a Internet. El usuario móvil puede cambiar de punto de acceso según la ubicación en la que esté y según qué punto de acceso ofrezca la mejor conexión. Al igual que en la telefonía móvil, los usuarios de WLAN tienen a su disposición una amplia red que no los ata a una ubicación concreta para acceder a ella. Hay más información detallada acerca de WLAN en la Sección 34.1, “LAN inalámbrica” (p. 649).

Bluetooth
: Bluetooth dispone del espectro más amplio de aplicaciones de todas las tecnologías inalámbricas. Bluetooth se puede utilizar para comunicar equipos entre sí (portátiles) y dispositivos PDA o teléfonos móviles, como sucede con IrDA. También se puede utilizar para conectar varios equipos dentro de una distancia visible. Bluetooth se utiliza igualmente para conectar entre sí componentes de sistemas inalámbricos, como teclados y ratones. El alcance de esta tecnología, sin embargo, no es suficiente para conectar sistemas remotos a una red. WLAN es la tecnología adecuada para comunicarse a través de obstáculos físicos como por ejemplo paredes. Hay más información sobre Bluetooth, sus aplicaciones y su configuración en la Sección 34.2, "Bluetooth" (p. 661).

IrDA
: IrDA es la tecnología inalámbrica de alcance más corto. Las dos partes comunicantes deben estar a una distancia visible la una de la otra. Obstáculos como paredes no pueden vencerse. Una posible aplicación de IrDA es la transmisión de archivos de un portátil a un teléfono móvil. El corto trayecto desde el portátil al teléfono móvil queda cubierto con IrDA. El transporte de largo alcance del archivo al receptor del archivo lo gestiona la red móvil. Otra posible aplicación de IrDA es la transmisión inalámbrica de trabajos de impresión en una oficina. Hay más información disponible sobre IrDA en la Sección 34.3, "Transmisión de datos mediante infrarrojos" (p. 673).

30.1.4 Seguridad de los datos

Lo ideal es que se protejan los datos del equipo portátil de varias maneras frente a accesos no autorizados. Se pueden tomar medidas de seguridad en las siguientes áreas:

Protección frente a robos
: En la medida de lo posible, asegure siempre su sistema físicamente frente a robos. Puede adquirir varios dispositivos de seguridad, como cadenas.

Seguridad de los datos del sistema
: Los datos clave no sólo deben estar cifrados al transmitirse, sino que también deben estar cifrados en el disco duro. Esto garantiza la seguridad en caso de robo. En la Sección 4.3, "Cifrado de particiones y archivos" (p. 127) se describe cómo crear una partición cifrada con SUSE Linux.

IMPORTANTE: Seguridad de los datos y suspensión en disco

Las particiones cifradas no se desmontan durante un evento de suspensión en disco. Por lo tanto, todos los datos de estas particiones quedarán a disposición de cualquiera que consiga robar el hardware y reanude el disco duro.

Seguridad de la red
: Siempre que se transfieran datos, independientemente de cómo se haga, debe hacerse de forma segura. Encontrará información sobre los problemas generales de seguridad relacionados con Linux y el uso de redes en la Sección 4.5, “Seguridad y confidencialidad” (p. 140). También se incluyen medidas de seguridad relacionadas con el uso de redes inalámbricas en el Capítulo 34, *Comunicación inalámbrica* (p. 649).

30.2 Hardware móvil

SUSE Linux admite la detección automática de dispositivos de almacenamiento móviles mediante Firewire (IEEE 1394) o USB. El término *dispositivo de almacenamiento móvil* se aplica a cualquier tipo de disco duro Firewire o USB, unidad flash USB o cámara digital. Estos dispositivos se detectan automáticamente y se configuran a través de HotPlug nada más conectarse al sistema mediante la interfaz correspondiente. subfs y submount garantizan que los dispositivos se monten en sus ubicaciones correspondientes en el sistema de archivos. El usuario queda totalmente libre de realizar las tareas de montaje y desmontaje manual que sí tenía que llevar a cabo en las versiones anteriores de SUSE Linux. Bastará con desconectar el dispositivo en cuanto el programa que lo estaba usando deje de acceder a él.

Discos duros externos (USB y Firewire)
: En cuanto el sistema reconozca correctamente el disco duro externo, aparecerá su icono en *My Computer* (Mi equipo) en KDE o en *Computer* (Equipo) en GNOME en la lista de unidades montadas. Al hacer clic en el icono se mostrará el contenido de la unidad. Aquí se podrán crear carpetas y archivos, así como editarlos y suprimirlos. Para cambiar el nombre que le haya dado el sistema al disco duro, seleccione el elemento de menú correspondiente en el menú que se abre al hacer clic con el botón derecho del ratón en el icono. El cambio de nombre sólo se aplica a su visualización en el gestor de archivos. El descriptor por el que está montado el dispositivo en `/media` permanece igual.

Unidades flash USB
: El sistema gestiona estos dispositivos como si fueran discos externos. Así, también es posible cambiar el nombre de las entradas en el gestor de archivos.

Cámaras digitales (USB y Firewire)
: Las cámaras digitales que reconoce el sistema también aparecen como unidades externas en la descripción del gestor de archivos. KDE permite leer las imágenes y acceder a ellas en la URL `camera:/`. Después, las imágenes se pueden procesar con Digikam o con The GIMP. Si se utiliza GNOME, Nautilus muestra las imágenes en sus propias carpetas. f-spot es una sencilla utilidad de gestión y procesamiento de imágenes. The GIMP permite realizar tareas de procesamiento fotográfico avanzadas. Para obtener más información sobre cámaras digitales y gestión de imágenes, consulte el Capítulo *Cámaras digitales y Linux* (↑Aplicaciones).

30.3 Teléfonos móviles y dispositivos PDA

Los sistemas de escritorio y los portátiles se pueden comunicar con los teléfonos móviles a través de Bluetooth o de IrDA. Algunos modelos admiten los dos protocolos, mientras que otros sólo uno de los dos. Las áreas de uso de los dos protocolos, así como la documentación correspondiente ampliada, ya se han mencionado en la "Comunicación inalámbrica" (p. 589). La configuración de estos protocolos, así como la de los teléfonos móviles en sí, se describe en sus respectivos manuales. La configuración del sistema Linux se describe en la Sección 34.2, "Bluetooth" (p. 661) y la Sección 34.3, "Transmisión de datos mediante infrarrojos" (p. 673).

Evolution y Kontact incluyen de fábrica la compatibilidad necesaria para sincronizarse con los dispositivos de mano fabricados por Palm, Inc. La conexión inicial con el dispositivo se lleva cabo fácilmente en ambos casos con la ayuda de un asistente. Una vez configurada la compatibilidad con una unidad Palm Pilot, habrá que determinar qué tipo de datos se deben sincronizar (direcciones, citas, etc.). Ambas aplicaciones de trabajo en grupo se describen en *Aplicaciones.*

El programa KPilot, tal como viene integrado en Kontact, también se puede adquirir como una utilidad independiente. Lo anterior se describe en *Aplicaciones.* El programa KitchenSync también puede utilizarse para sincronizar datos de direcciones.

30.4 Información adicional

El punto de referencia central para todas las preguntas relacionadas con dispositivos móviles y Linux es http://tuxmobil.org/. Dicho sitio Web incluye varias secciones dedicadas a aspectos de hardware y de software para portátiles, dispositivos PDA, teléfonos móviles y otro tipo de hardware móvil.

Un acercamiento parecido al de http://tuxmobil.org/ es el de http://www.linux-on-laptops.com/. Aquí podrá encontrar más información sobre portátiles y dispositivos de mano.

SUSE mantiene una lista de correo en alemán dedicada a portátiles. Consulte la http://lists.suse.com/archive/suse-laptop/. En esta lista, tanto usuarios como desarrolladores hablan sobre aspectos relacionados con la informática móvil y SUSE Linux. Si bien se dan respuestas en inglés, la mayoría de la información archivada está sólo en alemán.

Si tiene problemas de gestión de energía con SUSE Linux en equipos portátiles, se recomienda leer el archivo README (Léame) en /usr/share/doc/packages/powersave. Este directorio suele contener información de última hora publicada por desarrolladores e ingenieros de pruebas, por lo que proporciona útiles consejos para solucionar problemas.

31 PCMCIA

PCMCIA se utiliza con frecuencia para hacer referencia al hardware, aunque tiene su origen en la organización que estandarizó todos los tipos posibles de tarjetas PC, la *PC Memory Card International Association* (Asociación internacional de tarjetas de memoria para equipos personales). Al principio, PCMCIA sólo incluía las tarjetas PC (que utilizaban un bus de 16 bits como en las tarjetas ISA), pero posteriormente se incluyeron las tarjetas CardBus (que utilizaban un bus de 32 bits). Una amplia gama de hardware PCMCIA es compatible con Linux. Además, Linux incluye herramientas para gestionar PCMCIA.

Las tarjetas PCMCIA se utilizan principalmente en equipos móviles para una gran variedad de funciones. Por ejemplo:

- Adaptadores Ethernet y LAN inalámbricos
- Tarjetas Bluetooth
- Tarjetas de memoria (Flash, SRAM y otras)
- Adaptadores de tarjetas de memoria (SD, MMC, SmartMedia, CompactFlash o MemoryStick)
- Módems

La mayor parte de la gestión de las tarjetas se realiza de manera silenciosa mediante udev y hotplug. Cuando es necesario la acción del usuario, se utiliza el comando `pccardctl`. Para obtener información detallada de PCMCIA, consulte la Sección 31.2, "Descripción detallada de PCMCIA" (p. 597). Para obtener más información acerca del

comando `pccardctl`, consulte la Sección 31.1, “Control de las tarjetas PCMCIA mediante pccardctl” (p. 596).

31.1 Control de las tarjetas PCMCIA mediante pccardctl

La gestión de tarjetas se realiza normalmente mediante udev y hotplug sin ninguna intervención por parte del usuario. pccardctl permite el control manual de la tarjeta en caso de que el proceso automático no funcione perfectamente.

A continuación, encontrará una lista de los comandos pccardctl más importantes. Todos ellos deben ser ejecutados por el usuario Root:

`pccardctl insert`
: Si la tarjeta no se ha detectado automáticamente, sirve para notificar a los controladores del cliente que la tarjeta se acaba de insertar.

`pccardctl eject`
: Expulsa la tarjeta manualmente y notifica a los controladores del cliente sobre la expulsión. Además corta el suministro al zócalo. Esta opción es tremendamente útil si ha detectado problemas con la suspensión y reanudación, tal y como se describe en la Sección 31.3.2, “Problemas generales de suspensión con PCMCIA” (p. 602).

`pccardctl suspend`
: Apaga e interrumpe el suministro del zócalo, pero no expulsa la tarjeta (desasocia los módulos adecuados).

`pccardctl resume`
: Después de ejecutar el comando `pccardctl resume`, activa el suministro al zócalo y restaura la configuración que había antes del evento de `suspensión.`

Para obtener más información, consulte la página Man de pccardctl.

31.2 Descripción detallada de PCMCIA

En las secciones siguientes se describe lo que ocurre en el sistema Linux cuando un dispositivo PCMCIA se conecta al equipo. Los componentes interactúan unos con otros, por lo que es necesario cumplir muchos requisitos para que un dispositivo PCMCIA sea compatible.

Lo que a continuación se explica es una descripción somera del proceso de inicialización de PCMCIA en Linux:

1. El bridge PCMCIA (o zócalo) debe configurarse adecuadamente, tal y como se describe en la Sección 31.2.1, “Inicialización del bridge” (p. 598). Los requisitos previos son los siguientes:

   - Controlador adecuado para el bridge
   - Rangos adicionales de E/S y de memoria para las tarjetas PC

2. Una vez que el bridge se haya configurado adecuadamente, el controlador del bridge detecta la presencia de una tarjeta y activa su inicialización, tal y como se describe en la Sección 31.2.2, “Inicialización de la tarjeta” (p. 598):

   a. Determine el tipo de tarjeta.

   b. Proporcione el voltaje adecuado.

   c. Asigne los rangos de E/S y de memoria así como las líneas IRQ a la tarjeta.

   d. Active la inicialización de la tarjeta o del dispositivo asociando el controlador de tarjeta adecuado.

   e. En el caso de algunas tarjetas es necesario cargar la estructura de información de la tarjeta (CIS).

3. Por último, se configura la interfaz y se deja lista para su uso. Para obtener más información, consulte la Sección 31.2.3, “Configuración de la interfaz” (p. 600).

31.2.1 Inicialización del bridge

La mayoría de bridges PCMCIA son dispositivos PCI que se tratan como tales. El proceso de inicialización del bridge puede resumirse de la siguiente manera:

1. Hotplug crea un evento PCI.

2. udev llama a `/sbin/hwup` para cargar el controlador. `/sbin/hwup` comprueba `/etc/sysconfig/hardware` para ver si hay una configuración de dispositivos existente. Si se encuentra una configuración adecuada, se usará. En caso contrario, `/sbin/hwup` llamará a `modprobe` con la cadena `modalias` proporcionada por el núcleo para cargar el módulo del controlador.

3. Se enviarán nuevos eventos hotplug (uno por cada zócalo de PCMCIA).

4. Los pasos siguientes se omiten si sólo se usan tarjetas CardBus:

   a. Los eventos `pcmcia_socket` activan udev para que llame a `/sbin/hwup` y cargue el módulo del núcleo de `pcmcia`.

   b. Todos los rangos de memoria y de E/S especificados en `/etc/pcmcia/config.opts` se añadirán al zócalo.

   c. Los servicios de tarjeta en el núcleo comprobarán estos rangos. Si los rangos de memoria de `/etc/pcmcia/config.opts` no son correctos, este paso podría hacer que el equipo falle y se detenga. Consulte la Sección 31.3.1, “Detención del equipo por un fallo en PCMCIA” (p. 600) para obtener información sobre cómo depurar y solucionar este problema.

Una vez que se hayan completado correctamente estos pasos, el bridge se habrá inicializado completamente. Después de esto, la tarjeta se inicializa tal y como se describe en la sección siguiente:

31.2.2 Inicialización de la tarjeta

Los eventos provocados al conectar una tarjeta PCMCIA pueden resumirse de esta manera:

1. Se produce un evento hotplug. Para las tarjetas de PC, se trata de un evento `pcmcia`. Para las tarjetas CardBus, se trata de un evento `pci`.

2. Para cualquier evento, udev llama a `/sbin/hwup` para cargar el módulo del controlador. El nombre del módulo se especifica en un archivo `hwcfg*` de `/etc/sysconfig/hardware` o mediante `modprobe modalias`.

3. Si es necesario, la inicialización del dispositivo activa un evento hotplug de firmware, se busca el firmware y se carga.

4. El controlador del dispositivo registrará las interfaces.

Después de haber completado estos pasos, el sistema sigue con la configuración de la interfaz, tal y como se describe en la siguiente sección.

Si su tarjeta es PC, podrá necesitar algunos de los parámetros siguientes en `/etc/sysconfig/pcmcia` para que sea totalmente compatible y poder trabajar sin problemas:

`PCMCIA_LOAD_CIS`
: El firmware de la tarjeta PC se denomina *CIS* (Card Information Structure, Estructura de información de la tarjeta). Proporciona detalles de implementación adicionales de la tarjeta. El comando `hwup` comprueba la integridad del CIS incorporado de la tarjeta e intenta cargar otro a partir del disco, siempre y cuando el CIS de la tarjeta esté dañado. El ajuste por defecto es `yes` (sí). Para inhabilitar la carga de CIS del disco, defina la variable en `no`.

`PCMCIA_ALLOW_FUNC_MATCH`
: Los controladores del dispositivo para Linux contienen una tabla de ID de dispositivo que indica a los controladores los dispositivos que va a gestionar. Esto quiere decir que sólo serán compatibles aquellos dispositivos cuyos ID sean conocidos por el núcleo. Para que aquellas tarjetas cuyos ID no aparezcan sean compatibles, puede utilizar la coincidencia de funciones. Esto quiere decir que no se seleccionará el controlador por el ID, sino por la función de la tarjeta (como, por ejemplo, una tarjeta de red) y que sería responsable de cualquier tarjeta PC insertada con esa función (como las tarjetas de red). El ajuste por defecto es `yes` (sí). Para inhabilitar la coincidencia de funciones, defina esta variable en `no`.

`PCMCIA_COLDPLUG_REINSERT`
: En ocasiones ocurre que las tarjetas que se han insertado antes de arrancar no se detectan. Para evitarlo, provoque una expulsión y una inserción de software de la

tarjeta definiendo PCMCIA_COLDPLUG_REINSERT en yes (sí). El ajuste por defecto es no.

31.2.3 Configuración de la interfaz

Dependiendo del tipo de tarjeta, se registrarán interfaces distintas después de que se haya completado correctamente la inicialización. El registro de la interfaz se gestiona mediante el hotplug de udev. Para obtener más información acerca de udev y de hotplug, consulte el Capítulo 12, *Gestión dinámica de dispositivos de núcleo con udev* (p. 273).

31.3 Solución de problemas

A continuación hay una lista de los problemas más importantes que se producen a veces con PCMCIA. Hay más información sobre esto disponible en el archivo léame de PCMCIA (/usr/share/doc/packages/pcmciautils/README.SuSE).

31.3.1 Detención del equipo por un fallo en PCMCIA

Cuando se inicia PCMCIA al arrancar, se produce un fallo del equipo y éste se detiene. Para averiguar la causa de la detención del equipo, configúrelo manualmente tal y como se describe a continuación. Al configurar PCMCIA manualmente y con cuidado, podrá identificar claramente el paso o componente que ha provocado la detención del sistema. Una vez identificado el elemento culpable, podrá evitar el paso o componente problemático.

Para configurar manualmente PCMCIA, siga este procedimiento:

1. Evite que PCMCIA se inicie al arrancar el sistema y habilite SysRq para que la depuración sea más sencilla añadiendo las siguientes opciones tras el indicador de arranque:

   ```
   init=3 pcmcia=off sysrq=1
   ```

   Para obtener más información acerca de SysRq, consulte /usr/src/linux/Documentation/sysrq.txt.

2 Arranque el sistema en un entorno basado en texto e inicie la sesión como usuario Root.

3 Añada los módulos PCMCIA adecuados al núcleo:

```
/sbin/modprobe yenta_socket
/sbin/modprobe pcmcia
```

4 Inicie el zócalo PCMCIA:

```
/sbin/pcmcia-socket-startupN
```

Sustituya *N* por el número del zócalo. Repita este paso para cada zócalo.

5 Si el paso anterior ha provocado la detención del equipo, ha podido ser causado por rangos de memoria o de E/S erróneos especificados en `/etc/pcmcia/config.opts`. Para evitarlo, haga una de las acciones siguientes:

- Excluya rangos en `/ect/pcmcia/config.opts` y vuelva a intentar configurar el zócalo.
- Añada los rangos manualmente tal y como se describe a continuación.

  Después de añadir correctamente los rangos adecuados manualmente, defínalos permanentemente incluyéndolos en `/etc/pcmcia/config.opts`

6 Después de configurar el zócalo correctamente, la inicialización de la tarjeta y la configuración de la interfaz deben funcionar tal y como se describe en la Sección 31.2.2, “Inicialización de la tarjeta” (p. 598) y en la Sección 31.2.3, “Configuración de la interfaz” (p. 600).

Para añadir manualmente rangos de E/S, proceda de la siguiente manera (para cada zócalo):

1 Cambie al directorio que contiene las configuraciones de rango (en este caso `pcmcia_socket0`, adapte el número de zócalo según el caso):

```
cd /sys/class/pcmcia_socket/pcmcia_socket0
```

2 Ejecute el comando siguiente:

```
echo principio - fin > available_resources_io
```

Sustituya *principio* y *fin* por las direcciones en las que se debería iniciar y finalizar el nuevo rango. Los valores correctos sólo pueden determinarse siguiendo el método de prueba y error.

Añada manualmente los siguientes rangos:

```
echo 0x800 - 0x8ff > available_resources_io
echo 0xc00 - 0xcff > available_resources_io
```

es igual a la siguiente línea de `/etc/pcmcia/config.opts`:

```
include port 0x800-0x8ff, port 0xc00 0xcff
```

El mismo procedimiento se aplica a los rangos de memoria debajo de `available_resources_mem`.

IMPORTANTE: Identificación de los ajustes por defecto incorrectos

Si encuentra un rango incorrecto en el archivo de configuración por defecto (`/etc/pcmcia/config.opts`) incluido con el producto, envíe el error a `http://bugzilla.novell.com` para que los desarrolladores puedan solucionar el problema.

31.3.2 Problemas generales de suspensión con PCMCIA

Siempre que el sistema se encuentre en modo de suspensión (suspensión de disco, de RAM o en espera), no conecte o desconecte ningún elemento de hardware. De lo contrario, el sistema podría no reanudarse convenientemente.

Para expulsar automáticamente las tarjetas PCMCIA en suspensión, realice las siguientes acciones:

1. Inicie sesión como usuario Root.
2. Abra el archivo `/etc/powersave/sleep`.
3. Defina las variables siguientes:

```
SUSPEND2DISK_EJECT_PCMCIA="yes"
SUSPEND2RAM_EJECT_PCMCIA="yes"
STANDBY_EJECT_PCMCIA="yes"
```

4 Guarde el archivo para aplicar los ajustes.

Si es necesario expulsar módulos adicionales en suspensión, siga tal y como se ha especificado anteriormente y añada nombres de módulo a las variables siguientes:

```
UNLOAD_MODULES_BEFORE_SUSPEND2DISK=""
UNLOAD_MODULES_BEFORE_SUSPEND2RAM=""
UNLOAD_MODULES_BEFORE_STANDBY=""
```

Para obtener información general acerca del daemon powersave, consulte la Sección 33.5, “Paquete powersave” (p. 634).

31.3.3 Información adicional

Encontrará la información más actualizada acerca de PCMCIA en `/usr/share/doc/packages/pcmciautils/README.SuSE`. Para obtener una descripción general exhaustiva del hardware de PCMCIA y dónde se usa, visite el sitio Web de PCMCIA (`http://www.pcmcia.org/pccard.htm`). Si desea comprobar si una tarjeta o dispositivo determinado es compatible con Linux, consulte el informe sobre tarjetas PCMCIA/CF/CardBus en Linux *(Linux PCMCIA/CF/CardBus Card Survey)* en `http://tuxmobil.org/pcmcia_linux.html`.

Gestión de perfiles de la configuración del sistema

32

Con la ayuda de SCPM (gestión de perfiles de la configuración del sistema), adapte la configuración del equipo a los distintos entornos operativos o configuraciones de hardware. SCPM gestiona un conjunto de perfiles de sistema para las distintas situaciones. SCPM permite cambiar fácilmente entre perfiles de sistema, con lo que se elimina la necesidad de volver a configurar el sistema manualmente.

En algunas situaciones es necesario modificar la configuración del sistema. Este sería el caso de equipos móviles que están funcionando en distintas ubicaciones. Si un sistema de escritorio debe estar funcionando temporalmente con otros componentes de hardware distintos a los habituales, SCPM viene como anillo al dedo. La restauración de la configuración original del sistema debe ser sencilla y la modificación de la configuración del sistema debe poder reproducirse. Gracias a SCPM, cualquier parte de la configuración del sistema puede mantenerse en un perfil personalizado.

El campo principal de la aplicación de SCPM es la configuración en red de equipos portátiles. Las distintas configuraciones de red requieren con frecuencia ajustes diferentes de otros servicios como el correo electrónico o los alternos. También otros elementos, como las diferentes impresoras domésticas y de la oficina, la configuración personalizada del servidor X para el proyector multimedia en conferencias, ajustes especiales de ahorro de energía para cuando se esté de viaje o una zona horaria distinta en una subsidiaria en el extranjero.

32.1 Terminología

A continuación se explican algunos términos empleados en la documentación de SCPM y en el módulo YaST.

configuración del sistema
: Hace referencia a la configuración completa del equipo. Cubre todos los ajustes fundamentales, como el uso de particiones de disco duro, los ajustes de red, la selección de zona horaria y las asignaciones del teclado.

perfil o *perfil del sistema*
: Estado que se ha guardado y se puede recuperar en cualquier momento.

perfil activo
: Hace referencia al último perfil seleccionado. Esto no quiere decir que la configuración del sistema actual se corresponde exactamente con este perfil ya que puede modificarse la configuración en cualquier momento.

recurso
: Elemento que participa en la configuración del sistema. Puede ser un archivo o un enlace simbólico incluidos los metadatos (como el usuario), los permisos o el tiempo de acceso. También puede tratarse de un servicio del sistema que se ejecuta en este perfil pero que se desactiva en otro.

grupo de recursos
: Cada recurso pertenece a un *grupo de recursos* determinado. Estos grupos contienen todos los recursos que van juntos de manera lógica (la mayoría de grupos incluyen tanto un servicio como los archivos de configuración correspondientes). Es muy sencillo ensamblar los recursos gestionados por SCPM porque no exige ningún conocimiento de los archivos de configuración del servicio deseado. SCPM incorpora una selección de grupos de recursos preconfigurados que debería ser suficiente para la mayoría de situaciones.

32.2 Configuración de SCPM

Las siguientes secciones presentan la configuración de SCPM a través de un ejemplo real: un equipo portátil que se utiliza en varias redes distintas. Los principales retos a los que hay que hacer frente en esta situación son:

- Entornos de red cambiantes, como LAN inalámbrica en casa y Ethernet en el trabajo
- Distintas configuraciones de impresora en casa y en el trabajo

Para activar y ejecutar SCPM con el fin de gestionar la configuración del sistema cambiante, haga lo siguiente:

1. Añada el applet selector de perfiles al panel y configúrelo para que permita que el usuario cambie de perfil como se describe en la Sección 32.3.1, “Configuración del applet de panel selector de perfiles” (p. 608).
2. Configure SCPM mediante el módulo gestor de perfiles de YaST como se describe en la Sección 32.3.2, “Configuración de los ajustes básicos de SCPM” (p. 608).
3. Cree un perfil para cada una de las configuraciones distintas mediante SUMF (interfaz de usuario de gestión unificada de SCPM, del inglés SCPM Unified Management Front-End) como se describe en la Sección 32.3.3, “Creación de un perfil nuevo” (p. 611).
4. Cambie al perfil adecuado para cada situación como se describe en la Sección 32.3.4, “Cambio de perfiles” (p. 611).

Si prefiere controlar SCPM desde la interfaz de línea de comandos, consulte la Sección 32.4, “Configuración de SCPM mediante la línea de comando” (p. 614) para obtener información detallada.

32.3 Configuración de SCPM mediante una interfaz gráfica del usuario

Las siguientes secciones presentan las herramientas gráficas que se utilizan para controlar los ajustes de los perfiles.

32.3.1 Configuración del applet de panel selector de perfiles

Antes de utilizar el selector de perfiles para controlar la configuración del sistema, debe configurarlo para que se inicie automáticamente al iniciar la sesión:

- En GNOME, haga clic en el panel con el botón derecho y seleccione Profile Chooser (Selector de perfiles) en la lista de applets disponibles.
- En KDE, seleccione *System → Desktop Applet → Profile Chooser* (Sistema - Miniaplicación de escritorio - Selector de perfiles) para añadir el selector de perfiles al panel.

32.3.2 Configuración de los ajustes básicos de SCPM

Configure el comportamiento básico de SCPM a través de YaST.

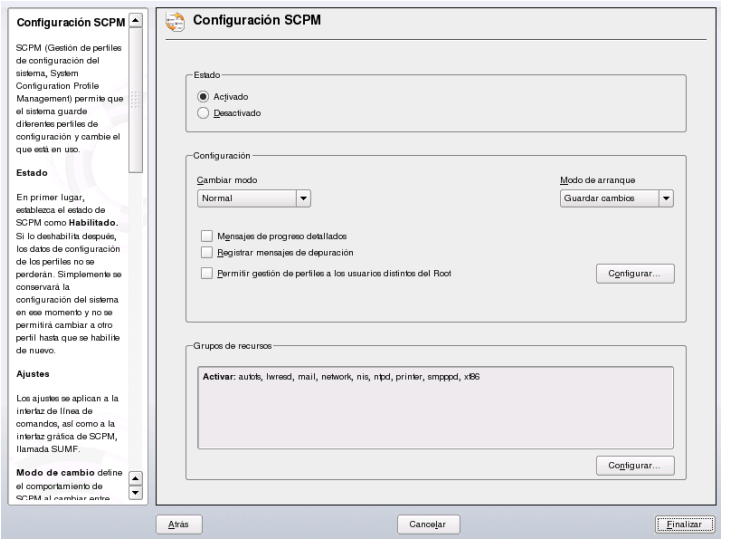
1. Inicie YaST desde el menú principal y seleccione el gestor de perfiles de YaST.
2. En *Gestión de perfiles de la configuración del sistema,* haga clic en *Opciones* y seleccione *Activado.*
3. Determine el nivel de detalle de SCPM seleccionando uno de los valores *Mensajes de progreso detallados* o *Registrar mensajes de depuración,* o ambos.
4. Determine el modo apropiado para cambiar de perfil de la configuración:
   - En caso de que quiera que SCPM muestre los recursos que se hayan modificado cuando se cambie a otro perfil y que guarde los cambios en el perfil activo, seleccione *Normal* o *Guardar cambios.*
   - Si quiere que SCPM descarte cualquier cambio en la configuración de los recursos cuando se cambie a otro perfil, seleccione *Desechar los cambios.*

5 Defina el modo de arranque y determine si los cambios en el perfil activo se deben guardar o si se deben descartar cuando el cambio de perfil se active en el momento del arranque.

6 Asegúrese de que todos los grupos de recursos que necesite estén incluidos en la selección activa, la cual se muestra en la sección *Grupos de recursos*. Si necesita grupos de recursos adicionales, utilice *Configurar recursos* para ajustarlos. Para obtener información detallada, consulte la Sección 32.3.6, “Configuración de grupos de recursos” (p. 613).

   En la situación de ejemplo, no tiene que configurar recursos adicionales, ya que los recursos de red y de impresora están incluidos por defecto.

Figura 32.1 *YaST: configuración básica de SCPM*



Para permitir que otros usuarios que no sean el Root gestionen los perfiles, haga lo siguiente:

1 Inicie YaST desde el menú principal y seleccione el gestor de perfiles de YaST.

2 Seleccione *Permitir que usuarios que no sean Root gestionen perfiles*. Consulte la Figura 32.2, “YaST: configuración de usuarios SCPM” (p. 610).

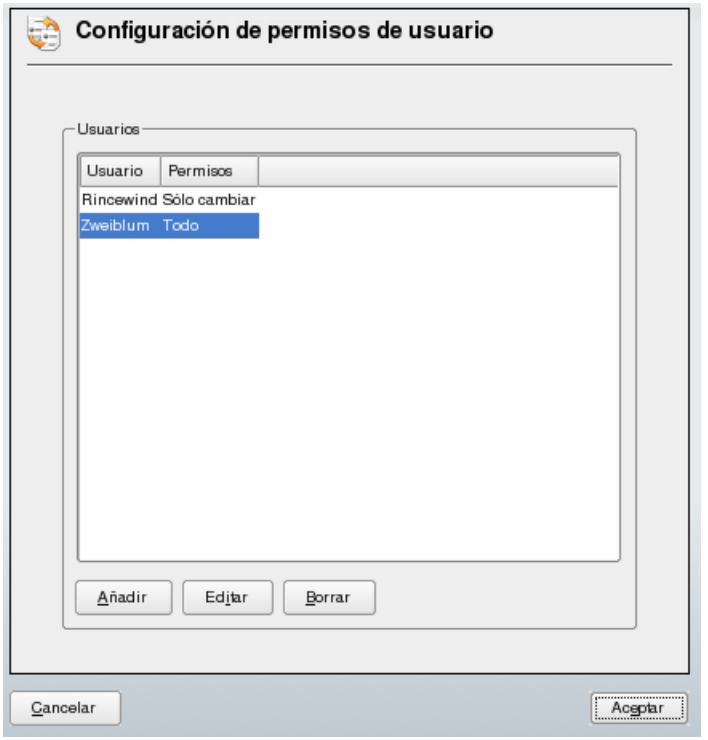
3 Haga clic en *Configurar usuarios.*

4 Haga clic en *Añadir* para agregar a los usuarios que deban tener la posibilidad de gestionar perfiles.

5 Con cada usuario, especifique si debe tener permiso para cambiar de perfil únicamente o para cambiar de perfil, modificar perfiles y crearlos.

6 Haga clic en *Aceptar* para aplicar los ajustes y cerrar YaST.

Figura 32.2 *YaST: configuración de usuarios SCPM*



32.3.3 Creación de un perfil nuevo

Tras habilitar SCPM, se incluye un perfil con el nombre `default` (por defecto) que incluye la configuración del sistema activa. Puede crear otro perfil que se ajuste a los requisitos de otra configuración.

Para añadir un perfil nuevo a partir de la configuración del sistema activa, haga lo siguiente:

1. Haga clic con el botón derecho en el selector de perfiles y elija *Ejecutar el gestor de perfiles (SUMF)*.
2. Seleccione *Perfiles* → *Añadir*.
3. Introduzca el nombre del nuevo perfil y haga clic en *Aceptar*.
4. Determine si el perfil nuevo debe ser el perfil activo.

   Si selecciona *Sí,* SCPM cambia al nuevo perfil inmediatamente después de que se haya creado.

En este ejemplo, haga lo siguiente:

1. En la configuración de casa, habilite SCPM.
2. Cambie el nombre del perfil `default` por un nombre más descriptivo iniciando SUMF y seleccionando *Perfiles* → *Editar* para escribir el nombre nuevo.
3. En la configuración de trabajo, inicie SUMF y cree el perfil para el entorno del sistema en el trabajo.

Cuando tenga todos los perfiles que necesite, estará listo para cambiar de uno a otro siempre que requiera una configuración del sistema distinta. El cambio de perfiles se describe en la Sección 32.3.4, “Cambio de perfiles” (p. 611).

32.3.4 Cambio de perfiles

Existen dos formas de cambiar los perfiles. Puede seleccionar un perfil nuevo durante el arranque o cambiar el perfil en el sistema en ejecución.

Para seleccionar un perfil durante el arranque, haga lo siguiente:

1. En la pantalla de arranque, pulse F2 para acceder al menú *Otras opciones*.
2. Pulse F3 para ver la lista de perfiles disponibles.
3. Utilice las teclas de flecha para seleccionar el perfil adecuado y pulse Intro

   El sistema arrancará con la configuración seleccionada.

Para cambiar el perfil en un sistema en ejecución, haga lo siguiente:

1. Asegúrese de que puede cambiar el perfil sin ser un usuario Root. Si no es así, consulte la Sección 32.3.2, “Configuración de los ajustes básicos de SCPM” (p. 608).
2. Haga clic en el applet de panel selector de perfiles.
3. Seleccione el perfil oportuno en el menú que se muestra mediante las teclas de flecha y pulse Intro

   SCPM comprueba si se ha modificado algún recurso y solicita que se confirme el cambio del perfil. Si se han realizado cambios en la configuración del sistema, SCPM pregunta si se deben conservar o descartar al cambiar a otro perfil.

32.3.5 Edición de perfiles

Para ajustar perfiles existentes a un entorno distinto, por ejemplo, si quiere cambiar la configuración de la impresora de la red doméstica, haga lo siguiente:

1. Cambie al perfil que quiera ajustar como se describe en la Sección 32.3.4, “Cambio de perfiles” (p. 611). En este ejemplo, debería elegir el perfil `casa`.
2. Cambie los recursos que se deban ajustar mediante el módulo de YaST adecuado. En este ejemplo, ejecute la configuración de impresoras de YaST.
3. Una vez que se hayan aplicado los cambios de configuración, SCPM pregunta si esos cambios se deben aplicar de forma permanente al perfil activo cuando se vuelva a cambiar de perfil.

SUGERENCIA: Cómo forzar una actualización de perfiles

Si quiere forzar la actualización del perfil activo, haga clic en él desde el menú de selección de perfiles del applet de panel selector de perfiles. De esta forma se recarga el perfil y se le pregunta si quiere aplicar los cambios de configuración o descartarlos.

32.3.6 Configuración de grupos de recursos

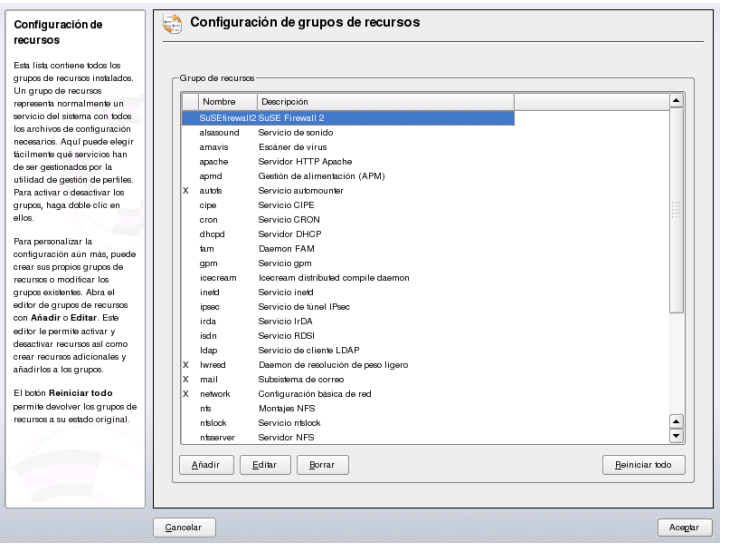
SCPM presenta un conjunto de grupos de recursos predefinidos que se incluyen en cualquier perfil por defecto. Sin embargo, en algunas situaciones es preciso incluir recursos y grupos de recursos adicionales.

Para cambiar la configuración de recursos o grupos de recursos, haga lo siguiente:

1. Inicie YaST desde el menú principal y el módulo gestor de perfiles de YaST.
2. En el cuadro de diálogo *Gestión de perfiles de la configuración del sistema,* haga clic en *Configurar recursos.*

   Se mostrarán todos los grupos de recursos del sistema disponibles, como se indica en la Figura 32.3, “Configuración de grupos de recursos” (p. 614).
3. Para añadir o editar un grupo de recursos:
   a. Defina o edite los valores de *Grupo de recursos* y *Descripción.*
   b. Introduzca los recursos adecuados (recursos, servicios o ambos) y suprima los que no necesite. Para restablecer el estado de los recursos seleccionados (descartar los cambios realizados y volver a los valores de configuración iniciales), elija *Reiniciar grupo.*
   c. Haga clic en *Aceptar* para salir de la configuración de recursos.
4. Haga clic en *Aceptar* para guardar los cambios realizados en el perfil activo.

Figura 32.3 *Configuración de grupos de recursos*



32.4 Configuración de SCPM mediante la línea de comando

En esta sección se explica la configuración de la línea de comandos de SCPM. Aprenda cómo iniciarla, configurarla y trabajar con perfiles.

32.4.1 Inicio de SCPM y definición de los grupos de recursos

SCPM debe activarse antes de usarse. Active SCPM mediante `scpm enable`. Cuando se ejecuta por primera vez, SCPM se inicializa, lo que tarda algunos segundos. Desactive SCPM con `scpm disable` en cualquier momento para impedir el cambio involuntario de perfiles. La reactivación posterior reanudará simplemente la inicialización.

Por defecto, SCPM gestiona los ajustes de red y de impresora además de la configuración de X.Org. Para gestionar servicios o archivos de configuración especiales, active los grupos de recursos respectivos. Para mostrar los grupos de recursos predefinidos, utilice

`scpm list_groups`. Para ver sólo los grupos ya activados, utilice `scpm list_groups -a`. Emita estos comandos como usuario `Root` en la línea de comando.

```
scpm list_groups -a

nis                 Cliente del Servicio de información de red (NIS)
mail                Subsistema de correo
ntpd                Daemon del protocolo horario de red (NTP)
xf86                Ajustes del servidor X
autofs              Servicio automounter
network             Ajustes básicos de red
printer             Ajustes de la impresora
```

Active o desactive un grupo con `scpm activate_group NOMBRE` o `scpm deactivate_group NOMBRE`. Sustituya `NOMBRE` con el nombre correspondiente del grupo.

32.4.2 Creación y gestión de perfiles

Ya existe un perfil denominado `default` después de activar SCPM. Obtenga una lista de todos los perfiles disponibles con `scpm list`. Este perfil existente también es el activo, lo que puede comprobarse mediante `scpm active`. El perfil `default` es una configuración básica desde la que derivan los otros perfiles. Por esta razón, todos los ajustes que deban ser idénticos en todos los perfiles deberían realizarse en primer lugar. A continuación, almacene estas modificaciones en el perfil activo con `scpm reload`. Se puede copiar o renombrar el perfil `default` como base para los nuevos perfiles.

Existen dos maneras de añadir un perfil. Si el perfil nuevo (al que llamaremos `trabajo`) debe basarse en el perfil `default`, créelo con `scpm copy default trabajo`. El comando `scpm switch trabajo` cambia al nuevo perfil, que ya podrá modificarse. Es posible que quiera modificar la configuración del sistema por algún motivo especial y guardar los cambios en un nuevo perfil. El comando `scpm add trabajo` crea un nuevo perfil al guardar la configuración actual del sistema en el perfil `trabajo` y al marcarlo como activo. Al ejecutar `scpm reload` se guardarán los cambios en el perfil `trabajo`.

Se pueden renombrar o suprimir los perfiles con los comandos `scpm rename x y` y `scpm delete z`. Por ejemplo, para renombrar `trabajo` a `proyecto`, introduzca `scpm rename trabajo proyecto`. Para suprimir `proyecto`, introduzca `scpm delete proyecto`. El perfil activo no puede suprimirse.

32.4.3 Cambio de perfiles de configuración

El comando `scpm switch trabajo` cambia a otro perfil (el perfil `trabajo`, en este caso). Cambie al perfil activo para incluir los ajustes modificados de la configuración del sistema en el perfil. Esto se corresponde con el comando `scpm reload`.

Al cambiar perfiles, SCPM comprueba primero los recursos del perfil activo que se han modificado. A continuación se le preguntará si la modificación de cada recurso debería añadirse al perfil activo o desecharse. Si prefiere una lista por separado de los recursos (tal y como ocurre en versiones anteriores de SCPM), utilice el comando de cambio con el parámetro `-r`: `scpm switch -r trabajo`.

```
scpm switch -r trabajo

Comprobación de los recursos modificados
Comprobación de los recursos que deben iniciarse/apagarse
Comprobación de dependencias
Restauración del perfil default
```

SCPM compara a continuación la configuración del sistema actual con el perfil al que cambiar. En esta fase, SCPM evalúa los servicios de sistema que deben detenerse o reiniciarse debido a las dependencias mutuas o para reflejar los cambios en la configuración. Es como un reinicio parcial del sistema que sólo concierne a una pequeña parte de éste mientras el resto continúa funcionando sin cambios. Sólo en este punto se detienen los servicios de sistema, todos los recursos modificados (como los archivos de configuración) se escriben y los servicios de sistema se reinician.

32.4.4 Ajustes avanzados de perfil

Puede introducir una descripción para cada perfil que se muestra con `scpm list`. Para el perfil activo, defínalo con `scpm set description "text"`. Escriba el nombre del perfil para los perfiles inactivos, por ejemplo, `scpm set description "text" trabajo`. En algunas ocasiones, podría ser conveniente realizar algunas acciones adicionales que no ofrece SCPM al cambiar perfiles. Interconecte hasta cuatro ejecutables por cada perfil. Se invocan en distintas fases del proceso de cambio. Estas fases se denominan:

Anterior a la detención
: Antes de detener los servicios al abandonar el perfil

Posterior a la detención
: Después de detener los servicios al abandonar el perfil

Anterior al inicio
: Antes de iniciar los servicios al activar el perfil

Posterior al inicio
: Después de iniciar los servicios al activar los perfiles

Inserte estas acciones con el comando `set` introduciendo `scpm set prestop filename`, `scpm set poststop filename`, `scpm set prestart filename` o `scpm set poststart filename`. Los guiones deben ser ejecutables y hacer referencia al intérprete correcto.

AVISO: Integración de un guión personalizado

El súperusuario (`Root`) debe poder leer y ejecutar los guiones adicionales que SCPM va a ejecutar. El acceso a estos archivos debe estar bloqueado para el resto de usuarios. Introduzca los comandos `chmod 700 filename` y `chown root:root filename` para proporcionar al usuario `Root` permisos exclusivos a los archivos.

Consulte todos los ajustes adicionales introducidos con `set` mediante `get`. El comando `scpm get poststart`, por ejemplo, devuelve el nombre de la llamada posterior al inicio o no devuelve nada si no se ha adjuntado nada. Restaure tales ajustes sobrescribiendo con `""`. El comando `scpm set prestop ""` elimina el programa anterior a la detención adjunto.

Pueden aplicarse todos los comandos `set` y `get` a un perfil arbitrario de la misma manera en que se han añadido los comentarios. Por ejemplo, `scpm get prestop filename trabajo` o `scpm get prestop trabajo`.

32.5 Solución de problemas

En esta sección se describen los problemas más frecuentes que se han detectado con SCPM. Aprenda cómo se producen y cómo puede resolverlos.

32.5.1 SCPM y NetworkManager

NetworkManager y SCPM comparten funcionalidad. Ambos se encargan de integrar los equipos en una red existente, ocultando al usuario esta transacción. NetworkManager funciona de forma dinámica y se adapta a cualquier entorno nuevo, mientras que SCPM se emplea para recuperar configuraciones del sistema definidas.

NetworkManager y SCPM no funcionan bien en paralelo, ya que NetworkManager no proporciona configuraciones que se puedan restaurar con SCPM. SCPM es excelente para aquellos que requieran configuraciones que se puedan restaurar; sin embargo, los usuarios privados que cambien con frecuencia de red (inalámbrica) deberían considerar la posibilidad de utilizar NetworkManager si la configuración de red es el único componente que se debe ajustar.

Si quiere utilizar SCPM para gestionar la configuración de red, deshabilite NetworkManager.

32.5.2 Terminación durante el proceso de cambio

En algunas ocasiones SCPM detiene el funcionamiento durante un procedimiento de cambio. Puede producirse debido a algún efecto exterior, como que el usuario lo aborte, un fallo de alimentación o incluso un error en el propio SCPM. Si esto ocurre, se mostrará un mensaje de error con información sobre el bloqueo de SCPM la próxima vez que inicie SCPM. El objetivo es proteger la seguridad del sistema, puesto que los datos almacenados en la base de datos pueden ser distintos de los del estado del sistema. Para resolver este problema, ejecute `scpm recover`. SCPM llevará a cabo todas las operaciones que faltaban de la ejecución anterior. También puede ejecutar `scpm recover -b`, que intentará deshacer todas las operaciones realizadas de la ejecución anterior. Si está utilizando el gestor de perfiles de YaST, obtenga un cuadro de diálogo de recuperación al inicio que le ofrezca la posibilidad de ejecutar los comandos descritos anteriormente.

32.6 Información adicional

La documentación más reciente está disponible en las páginas de información de SCPM (info scpm). La información para desarrolladores está disponible en `/usr/share/doc/packages/scpm`.

33 Gestión de energía

La gestión de energía es especialmente importante en el caso de los equipos portátiles, pero también es un aspecto importante en otros sistemas. Hay disponibles dos tecnologías: APM (gestión de energía avanzada, del inglés Advanced Power Management) y ACPI (interfaz avanzada de configuración y energía, del inglés Advanced Configuration and Power Interface). Además de estas tecnologías, también es posible ajustar la frecuencia de la CPU para ahorrar energía o reducir el ruido. Estas opciones se pueden configurar de forma manual o usando un módulo de YaST.

A diferencia de APM, que se usaba anteriormente en los equipos portátiles sólo para la gestión de energía, la información sobre el hardware y la herramienta de configuración de ACPI están disponibles en todos los equipos modernos (portátiles, equipos de sobremesa y servidores). Todas las tecnologías de gestión de energía requieren hardware adecuado y rutinas de BIOS. La mayoría de los portátiles y muchos de los equipos de sobremesa y los servidores modernos se ajustan a estos requisitos.

APM se utilizaba en muchos equipos antiguos. Dado que APM consiste en bastante medida en un conjunto de funciones implementado en el BIOS, el grado de compatibilidad con APM puede variar en función del hardware. Este hecho es aún más evidente en el caso de ACPI, ya que presenta una mayor complejidad. Por esta razón no tiene mucho sentido recomendar uno u otro sistema. Lo mejor que puede hacer es probar los distintos procedimientos con su hardware y elegir la tecnología con la que obtenga los mejores resultados.

IMPORTANTE: Gestión de energía en los procesadores AMD64

Los procesadores AMD64 con un núcleo de 64 bits sólo admiten el uso de ACPI.

33.1 Funciones de ahorro de energía

Las funciones de ahorro de energía no sólo son importantes para el uso móvil de los equipos portátiles, sino también para los sistemas de sobremesa. Las funciones principales y su uso en los sistemas de gestión de energía APM y ACPI son:

Stand-by
: En este modo de funcionamiento se apaga la pantalla. En algunos equipos, el rendimiento del procesador se puede limitar. Esta función no está disponible en todas las implementaciones APM, y se corresponde con los estados S1 o S2 de ACPI.

Suspender (volcado en la memoria)
: Este modo vuelca toda la información de estado del sistema en la memoria RAM. Posteriormente, todo el sistema (excepto la RAM) pasa a estar en reposo. En este estado, el equipo consume muy poca energía. La ventaja que ofrece es la posibilidad de reanudar el trabajo en el mismo punto en el que se dejó en sólo unos segundos, sin necesidad de arrancar y reiniciar las aplicaciones. Los dispositivos que utilizan APM se pueden suspender normalmente cerrando la cubierta del portátil y se activan al volver a abrirla. Esta función se corresponde con el estado S3 de ACPI. La compatibilidad con este estado está todavía en desarrollo y, en consecuencia, depende en gran medida del hardware.

Hibernación (volcado en el disco)
: En este modo de funcionamiento, todo el estado del sistema se vuelca en el disco duro y el sistema se apaga. Debe existir una partición swap del mismo tamaño al menos que la RAM para escribir todos los datos activos. La reactivación para salir de este estado puede requerir entre 30 y 90 segundos y se vuelve al estado previo a la suspensión. Algunos fabricantes ofrecen variantes de este modo como, por ejemplo, la función RediSafe de los Thinkpads de IBM. En ACPI el estado que se corresponde con la hibernación es el S4. En Linux, el volcado de la información en el disco se realiza mediante rutinas del núcleo que son independientes de APM y de ACPI.

Monitorización de la batería
: ACPI y APM comprueban la carga de la batería y proporcionan la información correspondiente. Además, ambos sistemas coordinan las acciones que se deben llevar a cabo cuando se alcanza un nivel de carga preocupante.

Desconexión automática
: Después de apagar, el equipo se desconecta. Esto es especialmente importante cuando se realiza un apagado automático justo antes de que se agote la batería.

Apagado de los componentes del sistema
: Desconectar el disco duro es el aspecto que ahorra más energía en todo el sistema. En función de la fiabilidad de todo el sistema, el disco duro puede ponerse en reposo durante algún tiempo. Sin embargo, el riesgo de perder datos aumenta a medida que incrementa el período de reposo. Otros componentes, como los dispositivos PCI que pueden llevarse a un estado especial de ahorro de energía, se pueden desactivar con ACPI (al menos en teoría) o inhabilitar de forma permanente desde la configuración del BIOS.

Control de la velocidad del procesador
: En lo que respecta a la CPU, se puede ahorrar energía de estas tres formas: se puede ajustar la frecuencia y el voltaje (PowerNow! o Speedstep), se pueden establecer limitaciones en la CPU y se puede poner el procesador en reposo (estados C). Dependiendo del modo de funcionamiento del equipo, estos métodos se pueden combinar también entre sí.

33.2 APM

Algunas de las funciones de ahorro de energía las realiza el propio BIOS APM. En muchos equipos portátiles, se pueden activar los estados stand-by y suspensión usando una combinación de teclas o cerrando la cubierta sin ninguna función de sistema operativo especial. Sin embargo, para activar estos modos con un comando, se deben realizar ciertas acciones antes de que el sistema entre en suspensión. Para ver el nivel de carga de la batería, se necesitan paquetes de programas especiales y un núcleo adecuado.

Los núcleos de SUSE Linux llevan incorporada la compatibilidad con APM. Sin embargo, APM se activa sólo si ACPI no está implementada en el BIOS y si se detecta un BIOS APM. Para activar la compatibilidad con APM, ACPI debe desactivarse usando `acpi=off` en el indicador de arranque. Especifique `cat /proc/apm` para comprobar

si APM está activa. Se mostrará un resultado compuesto por varios números para indicar que todo es correcto. Ahora puede apagar el equipo usando el comando `shutdown -h`.

Las implementaciones del BIOS que no sean totalmente estándares pueden provocar problemas con APM. Algunos de estos problemas se pueden evitar usando parámetros de arranque especiales. Todos los parámetros se introducen en el indicador de arranque con el formato `apm=`*`parámetro`*. El *`parámetro`* corresponde a uno de los siguientes:

on/off
: Habilita o inhabilita la compatibilidad con APM.

(no-)allow-ints
: Permite que se produzcan interrupciones durante la ejecución de las funciones del BIOS.

(no-)broken-psr
: La función "GetPowerStatus" del BIOS no funciona correctamente.

(no-)realmode-power-off
: Restablece el procesador al modo normal antes del apagado.

(no-)debug
: Registra los eventos de APM en el registro del sistema.

(no-)power-off
: Desconecta el sistema después de un apagado.

bounce-interval=*n*
: Tiempo (en centésimas de segundo) después de un evento de suspensión durante el cual se hace caso omiso de otros eventos de suspensión adicionales.

idle-threshold=*n*
: Porcentaje de inactividad del sistema a partir del cual se ejecuta la función de BIOS `idle` (0=siempre, 100=nunca).

idle-period=*n*
: Tiempo (en centésimas de segundo) después del cual se mide la actividad del sistema.

El daemon de APM (apmd) ha dejado de utilizarse. Sus funciones las gestiona ahora el nuevo daemon powersaved, que también es compatible con ACPI y proporciona muchas otras funciones.

33.3 ACPI

ACPI se ha diseñado para hacer posible que el sistema operativo configure y controle los componentes de hardware individuales. ACPI sustituye a los sistemas anteriores PnP y APM. Proporciona información acerca de la batería, el adaptador de CA, la temperatura, el ventilador y los eventos del sistema como, por ejemplo, que se debe cerrar la cubierta o que la batería está baja.

El BIOS proporciona tablas que contienen información acerca de los métodos de acceso al hardware y a los componentes individuales. El sistema operativo se sirve de esta información para tareas como la asignación de interrupciones o la activación y desactivación de componentes. Como el sistema operativo ejecuta los comandos almacenados en el BIOS, el funcionamiento depende de la implementación del BIOS. Las tablas que ACPI puede detectar y cargar se indican en `/var/log/boot.msg`. Consulte la Sección 33.3.4, “Solución de problemas” (p. 631) para obtener más información acerca de la resolución de los problemas de ACPI.

33.3.1 Activación de ACPI

Si el núcleo detecta un BIOS ACPI al arrancar el sistema, ACPI se activa automáticamente y APM se desactiva. El parámetro de arranque `acpi=force` puede ser necesario para algunas máquinas antiguas. El equipo debe ser compatible con ACPI 2.0 o posterior. Consulte los mensajes de arranque del núcleo en `/var/log/boot.msg` para ver si ACPI está activada.

A continuación, es necesario cargar una serie de módulos, de lo que se ocupa el guión de inicio de acpid. Si alguno de estos módulos causa problemas, puede impedirse su carga o descarga en `/etc/sysconfig/powersave/common`. En el registro del sistema (`/var/log/messages`) se encuentran los mensajes de los módulos, lo que le permite ver qué componentes se han detectado.

En `/proc/acpi` aparecen ahora varios archivos que informan sobre el estado del sistema o que se pueden usar para modificar algunos de los estados. Algunas funciones

no están totalmente operativas, ya que se encuentran todavía en desarrollo y el uso de otras depende en gran medida de la implementación del fabricante.

Todos los archivos (excepto `dsdt` y `fadt`) se pueden leer con `cat`. En algunos archivos, los ajustes se pueden modificar con `echo`; por ejemplo, `echo X > archivo` permite especificar los valores adecuados para X. Entre las posibilidades para acceder fácilmente a esos valores, se encuentra el comando `powersave`, que actúa como interfaz del daemon Powersave. A continuación, se describen los archivos más importantes:

`/proc/acpi/info`
: Información general acerca de ACPI.

`/proc/acpi/alarm`
: Aquí se especifica cuándo debe activarse el sistema después de haber estado en reposo. Por ahora, esta función no se admite totalmente.

`/proc/acpi/sleep`
: Proporciona información acerca de los posibles estados de reposo.

`/proc/acpi/event`
: Aquí se registran los eventos y el daemon Powersave los procesa (`powersaved`). Si ningún daemon accede a este archivo, los eventos (como, por ejemplo, presionar el botón de encendido o cerrar la cubierta) se podrán leer con `cat /proc/acpi/event` (se sale de ellos con Ctrl + C).

`/proc/acpi/dsdt` y `/proc/acpi/fadt`
: Estos archivos contienen las tablas ACPI DSDT (tabla de descripción de sistemas diferenciados, del inglés Differentiated System Description Table) y FADT (tabla de descripción de ACPI fija, del inglés Fixed ACPI Description Table). Dichas tablas pueden leerse con `acpidmp`, `acpidisasm` y `dmdecode`. Puede encontrar estos programas junto con la correspondiente documentación en el paquete `pmtools`, por ejemplo, `acpidmp DSDT | acpidisasm`.

`/proc/acpi/ac_adapter/AC/state`
: Muestra si está conectado el adaptador de CA.

`/proc/acpi/battery/BAT*/{alarm,info,state}`
: Información detallada sobre el estado de la batería. Para conocer el nivel de carga, es necesario comparar el valor de `last full capacity` (última capacidad total) de `info` (información) con el de `remaining capacity` (capacidad

restante) de `state` (estado). Una forma más fácil de hacerlo es usar alguno de los programas especiales que se describen en la Sección 33.3.3, "Herramientas de ACPI" (p. 631). El nivel de carga que provocará que se desencadene un evento de batería (como indicaciones de advertencia, de batería baja o de estado crítico) se puede especificar en `alarm` (alarma).

`/proc/acpi/button`
: Este directorio contiene información acerca de distintos commutadores, como los que corresponden a la cubierta y los botones del portátil.

`/proc/acpi/fan/FAN/state`
: Muestra si el ventilador está funcionando en ese momento. Puede activar o desactivar el ventilador automáticamente escribiendo en este archivo `0` (encender) o `3` (apagar). No obstante, tanto el código ACPI del núcleo como el hardware (o el BIOS) hacen caso omiso de este ajuste cuando la temperatura del sistema es demasiado elevada.

`/proc/acpi/processor/*`
: Se crea un subdirectorio independiente para cada CPU incluida en el sistema.

`/proc/acpi/processor/*/info`
: Información sobre las posibilidades de ahorro de energía del procesador.

`/proc/acpi/processor/*/power`
: Información sobre el estado actual del procesador. Un asterisco junto a `C2` significa que el procesador está inactivo, que es el estado más frecuente, como puede apreciarse por el valor de `usage` (uso).

`/proc/acpi/processor/*/throttling`
: Se puede utilizar para limitar el reloj del procesador. Normalmente, esto se puede hacer en 8 niveles. Esta opción es independiente del ajuste de la frecuencia de la CPU.

`/proc/acpi/processor/*/limit`
: Si el rendimiento (obsoleto) y las limitaciones se controlan de forma automática mediante un daemon, se pueden especificar aquí los límites máximos. Existen algunos límites fijados por el sistema y otros establecidos por el usuario.

`/proc/acpi/thermal_zone/`
: Hay un subdirectorio independiente para cada zona térmica. Una zona térmica es un área con propiedades térmicas semejantes, cuyo número y nombre están

diseñados por el fabricante del hardware. No obstante, muchas de las posibilidades que ofrece ACPI no se llegan a implementar nunca. En su lugar, el BIOS se ocupa normalmente de controlar la temperatura sin que el sistema operativo intervenga, ya que lo que está en juego aquí es la duración del hardware. En consecuencia, algunos de los archivos siguientes sólo tienen valor en la teoría.

`/proc/acpi/thermal_zone/*/temperature`
: La temperatura actual de la zona térmica.

`/proc/acpi/thermal_zone/*/state`
: El estado indica si todo está en orden (`ok`) o si ACPI refrigera de forma `active` (activa) o `passive` (pasiva). En los casos en los que el control del ventilador no depende de ACPI, el estado es siempre `ok`.

`/proc/acpi/thermal_zone/*/cooling_mode`
: Seleccione el método de refrigeración controlado por ACPI. Puede optar por el modo pasivo (menor rendimiento pero más económico) o por el activo (máximo rendimiento, pero el ventilador hace ruido).

`/proc/acpi/thermal_zone/*/trip_points`
: Permite establecer la temperatura a partir de la cual se deben realizar acciones específicas en el equipo como, por ejemplo, la refrigeración activa o pasiva, la suspensión (cuando el estado es `hot` [caliente]) o el apagado (cuando el estado es `critical` [crítico]). Las acciones posibles se encuentran definidas en DSDT en función del dispositivo. Los puntos que se determinan en la especificación ACPI son: `critical` (crítico), `hot` (caliente), `passive` (pasivo), `active1` (activo1) y `active2` (activo2). Aunque no estén implementados todos ellos, es necesario especificarlos en este orden en el archivo. Por ejemplo, la entrada `echo 90:0:70:0:0 > trip_points` asigna a la temperatura un valor `critical` (crítico) de `90` grados y un valor `passive` (pasivo) de `70` grados (todas las temperaturas se miden en grados Celsius).

`/proc/acpi/thermal_zone/*/polling_frequency`
: Si el valor de `temperature` (temperatura) no se actualiza automáticamente cuando cambia la temperatura, puede cambiar al modo de sondeo aquí. El comando `echo X > /proc/acpi/thermal_zone/*/polling_frequency` hace que se consulte la temperatura cada `X` segundos. Si `X=0` se inhabilitará el sondeo.

Las opciones de configuración, la información y los eventos mencionados no requieren una edición manual. Para ello, se puede utilizar el daemon Powersave (powersaved) y

sus distintas interfaces, como powersave, kpowersave y wmpowersave. Consulte la Sección 33.3.3, “Herramientas de ACPI” (p. 631).

33.3.2 Control del rendimiento de la CPU

Existen tres métodos de ahorro de energía para la CPU. Dependiendo del modo de funcionamiento del equipo, estos métodos se pueden combinar también entre sí. El ahorro de energía también significa que el sistema se calienta menos y, por lo tanto, el ventilador debe activarse con menos frecuencia.

Ajuste de la frecuencia y el voltaje
: PowerNow! y Speedstep son los nombres que han establecido las empresas AMD e Intel para esta tecnología que, por otra parte, incorporan también los procesadores de otros fabricantes. Este método consiste en reducir conjuntamente la frecuencia del reloj de la CPU y su voltaje central, con lo cual se consigue un ahorro de energía superior al lineal. Esto significa que con la mitad de la frecuencia (es decir, a medio rendimiento) se requiere mucho menos de la mitad de energía. Esta tecnología es independiente de APM y de ACPI. Existen dos métodos principales para ajustar la frecuencia de la CPU: a través del núcleo en sí o mediante una aplicación del espacio de usuario. Existen por tanto distintos gobernadores del núcleo que se pueden definir en `/sys/devices/system/cpu/cpu*/cpufreq/`.

  gobernador userspace
  : Si se define el gobernador userspace, el núcleo otorga el control del ajuste de frecuencia de la CPU a una aplicación del espacio de usuario, por lo general un daemon. En las distribuciones de SUSE Linux, este daemon es el paquete `powersaved`. Cuando se emplea esta implementación, la frecuencia de la CPU se ajusta en relación con la carga del sistema de cada momento. Por defecto se emplea una de las implementaciones del núcleo. No obstante, en algunos tipos de hardware o según procesadores o controladores específicos, la implementación del espacio de usuario es la única solución que funciona por el momento.

  gobernador ondemand
  : Se trata de la implantación en el núcleo de una directiva de frecuencia de la CPU dinámica que tendría que funcionar en la mayoría de sistemas. Cuado se detecta una carga alta en el sistema, la frecuencia de la CPU se aumenta inmediatamente, y se reduce con una carga baja del sistema.

gobernador conservative
: Este gobernador es similar a la implementación ondemand, con la excepción de que se emplea una directiva más conservadora. La carga del sistema puede ser alta durante un periodo de tiempo concreto antes de que se aumente la frecuencia de la CPU.

gobernador powersave
: La frecuencia de la CPU se define con el valor más bajo posible en términos estadísticos.

gobernador performance
: La frecuencia de la CPU se define con el valor más alto posible en términos estadísticos.

Limitación de la frecuencia del reloj
: Esta tecnología consiste en omitir un porcentaje determinado de los impulsos de la señal del reloj para la CPU. Con una limitación del 25%, se omite uno de cada cuatro impulsos; mientras que con una reducción del 87,5%, sólo uno de cada ocho impulsos llega al procesador. No obstante, el ahorro de energía es algo menor que el lineal. Normalmente, esta técnica se aplica solamente cuando no está disponible el ajuste de la frecuencia o para lograr el máximo ahorro de energía. Por otra parte, esta técnica requiere un proceso propio que la controle. La interfaz del sistema es `/proc/acpi/processor/*/throttling`.

Cómo poner el procesador en reposo
: El sistema operativo pone el procesador en estado de reposo cuando no hay ningún tipo de actividad. En este caso, el sistema operativo envía a la CPU el comando `halt`. Existen tres niveles: C1, C2 y C3. En el estado de máximo ahorro de energía (C3), se detiene incluso la sincronización del caché del procesador con la memoria principal, por lo que este estado se adopta únicamente cuando no existe ningún dispositivo que modifique el contenido de la memoria principal a través de la actividad maestra del bus. Algunos controladores no permiten el uso de C3. El estado actual se muestra en `/proc/acpi/processor/*/power`.

El ajuste de la frecuencia y las limitaciones son sólo relevantes cuando el procesador está ocupado, ya que, si éste se encuentra inactivo, se utiliza de todas formas el estado C más económico. Si la CPU está ocupada, el ajuste de la frecuencia es el mejor método para ahorrar energía. A menudo, el procesador no trabaja al máximo de su capacidad y basta con bajar su frecuencia. Normalmente, el método más adecuado consiste en un ajuste dinámico de la frecuencia por medio del gobernador ondemand del núcleo o de

un daemon, como powersaved. Cuando el equipo funciona con baterías o debe mantener una baja temperatura y hacer poco ruido, se recomienda establecer un ajuste estático a baja frecuencia.

La función de limitación debería utilizarse como último recurso, por ejemplo, para prolongar el tiempo de funcionamiento con baterías a pesar de que el sistema esté trabajando a pleno ritmo. No obstante, algunos sistemas no funcionan correctamente si la limitación aplicada es demasiado estricta. Por otra parte, la limitación de la CPU no sirve de nada cuando ésta tiene poca actividad.

En SUSE Linux, estas técnicas se controlan a través del daemon powersave. La configuración se describe en la Sección 33.5, “Paquete powersave” (p. 634).

33.3.3 Herramientas de ACPI

ACPI cuenta con una serie de herramientas más o menos completas. Entre ellas se encuentran las herramientas puramente informativas que muestran el estado de la batería o la temperatura (acpi, klaptopdaemon, wmacpimon, etc.); las que facilitan el acceso a estructuras en `/proc/acpi`; las que ayudan a monitorizar cambios (akpi, acpiw o gtkacpiw) y, por último, las que permiten editar las tablas ACPI en el BIOS (paquete `pmtools`).

33.3.4 Solución de problemas

Se puede distinguir entre dos tipos de problemas. Por una parte, puede haber fallos en el código ACPI del núcleo que no se hayan detectado a tiempo. En este caso, se proporcionará una solución para que la descargue. Los otros problemas son los más frecuentes: los que están causados por el BIOS. En algunos casos, se integran a propósito en el BIOS desviaciones de las especificaciones de ACPI para evitar fallos en la implementación ACPI en otros sistemas operativos de uso extendido. Existen también componentes de hardware con fallos graves en la implementación ACPI, por lo que se han incluido en una "lista negra" para impedir que el núcleo de Linux utilice en ellos ACPI.

Si surgen problemas, en primer lugar se debe actualizar el BIOS. Si el equipo no arrancar en absoluto, pruebe a utilizar algunos de los siguientes parámetros de arranque:

pci=noacpi
: No utilizar ACPI para configurar los dispositivos PCI.

acpi=oldboot
: Ejecutar sólo una configuración de recursos simples. No utilizar ACPI para otros propósitos.

acpi=off
: Inhabilita la ACPI.

AVISO: Problemas al arrancar sin ACPI

Algunos equipos nuevos, especialmente los sistemas SMP y AMD64, requieren ACPI para que el hardware se configure correctamente. Por lo tanto, el desactivar ACPI puede ocasionar problemas.

Monitorice los mensajes de arranque del sistema con el comando `dmesg | grep -2i acpi` después del arranque. También puede monitorizar todos los mensajes, ya que puede que el problema no esté causado por ACPI. Si ocurre un error durante el análisis de una tabla ACPI, la tabla más importante (que es DSDT) se puede sustituir por una versión mejorada. En estas circunstancias, se hace caso omiso de la tabla DSDT defectuosa del BIOS. El procedimiento se describe en la Sección 33.5.4, “Solución de problemas” (p. 641).

En la configuración del núcleo existe un conmutador para activar los mensajes de depuración de ACPI. Si se ha compilado e instalado un núcleo con depuración ACPI, esta información detallada puede servir de ayuda a los técnicos que traten de identificar el error.

Si se producen problemas con el hardware o el BIOS, es aconsejable ponerse en contacto con los fabricantes. A menudo, los fabricantes no proporcionan asistencia si se trata de Linux, por lo que es importante que tomen conciencia de los distintos problemas. No se tomarán el asunto en serio hasta que se den cuenta de que un número importante de sus clientes utiliza Linux.

Información adicional

Puede obtener información adicional y material de ayuda sobre ACPI:

- http://www.cpqlinux.com/acpi-howto.html (información detallada sobre procedimientos de ACPI y revisiones para DSDT)
- http://www.intel.com/technology/iapc/acpi/faq.htm (preguntas frecuentes sobre ACPI de @Intel)
- http://acpi.sourceforge.net/ (el proyecto ACPI4Linux en Sourceforge)
- http://www.poupinou.org/acpi/ (revisiones de DSDT de Bruno Ducrot)

33.4 Detención del disco duro

En Linux, es posible poner completamente en reposo el disco duro cuando no se necesita o hacer que funcione en modo silencioso o de ahorro de energía. En los equipos portátiles modernos, no es necesario desactivar manualmente los discos duros, ya que éstos adoptan por sí mismos el modo de ahorro de energía cuando no se necesitan. Sin embargo, si desea ahorrar el máximo de energía, puede probar algunos de los siguientes métodos. Casi todas las funciones se controlan con powersaved y el módulo de gestión de energía de YaST, que se describe con mayor profundidad en la Sección 33.6, “Módulo de gestión de energía de YaST” (p. 644).

La aplicación hdparm se utiliza para modificar los distintos ajustes del disco duro. La opción `-y` hace que el disco duro pase inmediatamente al modo stand-by, mientras que `-Y` lo pone en reposo. La opción `hdparm -S x` hace que el disco duro se apague tras un determinado período de inactividad. Puede asignar los siguientes valores a *x*: `0` apaga el mecanismo, por lo que el disco duro sigue ejecutándose continuamente. Los valores entre `1` y `240` se multiplican por 5 segundos. Los valores entre `241` y `251` se corresponden con 30 minutos entre 1 y 11 veces.

Las posibilidades internas de ahorro de energía del disco duro se controlan mediante la opción `-B`. Seleccione un valor entre `0` y `255`: el mayor ahorro de energía es el 0 y el rendimiento máximo es el 255. El resultado dependerá del disco duro que se use y es difícil de evaluar. Para que el disco duro sea más silencioso, use la opción `-M`. Seleccione un valor entre `128` y `254` para definir un estado entre silencioso (128) y rápido (254).

Sin embargo, a menudo no es fácil poner en reposo el disco duro, puesto que Linux cuenta con numerosos procesos que escriben datos en él, por lo que lo activan constantemente. En consecuencia, es importante conocer la forma en que Linux gestiona

los datos que deben escribirse en el disco duro. En primer lugar, todos los datos se almacenan en un buffer en la memoria RAM. El daemon de actualización del núcleo (kupdated) se encarga de monitorizar este buffer. Cuando los datos alcancen una determinada antigüedad o cuando el buffer esté lleno hasta un nivel concreto, los datos se pasarán al disco duro. El tamaño del buffer es dinámico y depende del tamaño de la memoria y de la carga del sistema. Por defecto, kupdated está configurado para funcionar a pequeños intervalos y conseguir así la mayor integridad de datos posible. Comprueba el buffer cada 5 segundos e informa al daemon bdflush si hay datos cuya antigüedad sea superior a los 30 segundos o si el buffer ha alcanzado un nivel de llenado del 30%. Entonces, el daemon bdflush escribe los datos en el disco duro, aunque también lo hace independientemente de kupdated si, por ejemplo, el buffer está lleno.

AVISO: Problemas con la integridad de los datos

Hacer cambios en los ajustes del daemon de actualización del núcleo puede poner en peligro la integridad de los datos.

Además de estos procesos, los sistemas de archivos llamados "journaling", como ReiserFS y Ext3, escriben sus metadatos en el disco duro con independencia de bdflush, lo cual también impide que el disco duro quede inactivo. Para evitarlo, se ha desarrollado una ampliación del núcleo específica para dispositivos móviles. Consulte `/usr/src/linux/Documentation/laptop-mode.txt` para obtener más información.

Otro elemento importante es la forma en que se comportan los programas activos. Por ejemplo, los editores de texto de calidad escriben periódicamente en el disco duro copias de seguridad del archivo que se esté modificando, lo que hace que el disco se reactive. Estas funciones se pueden desactivar, aunque ello va en detrimento de la integridad de los datos.

En este contexto, el daemon de correo postfix utiliza la variable `POSTFIX_LAPTOP`. Si esta variable está definida como `yes` (sí), postfix accederá al disco duro con menor frecuencia. No obstante, este hecho carece de importancia si el intervalo de kupdated se ha aumentado.

33.5 Paquete powersave

El paquete `powersave` se ocupa de todas las funciones de ahorro de energía mencionadas anteriormente. Debido a la creciente demanda general de un menor consumo de

energía, algunas de sus funciones son importantes también en estaciones de trabajo y servidores, como las funciones de suspensión, stand-by y ajuste de la frecuencia de CPU.

Este paquete incorpora todas las funciones de ahorro de energía del equipo y es compatible con cualquier hardware que utilice ACPI, APM, discos duros IDE y las tecnologías PowerNow! y SpeedStep. Todas las prestaciones de los paquetes `apmd`, `acpid`, `ospmd` y `cpufreqd` (ahora`cpuspeed`) se han agrupado ahora en el paquete `powersave`.. Los daemons de estos paquetes, con la excepción de acpid que actúa como multiplexor de los eventos de acpi, no se deben ejecutar al mismo tiempo que el daemon powersave.

Incluso aunque el sistema no disponga de todos los componentes de hardware mencionados anteriormente, se recomienda utilizar el daemon de powersave para regular la función de ahorro de energía. Como ACPI y APM se excluyen mutuamente, sólo podrá usar uno de ellos en su equipo. El daemon detecta automáticamente cualquier cambio en la configuración del hardware.

33.5.1 Configuración del paquete powersave

La configuración de powersave está distribuida en varios archivos. Cada opción de configuración contenida en ellos incluye documentación adicional acerca de su funcionalidad.

`/etc/sysconfig/powersave/common`
: Este archivo contiene ajustes generales para el daemon powersave. Por ejemplo, se puede obtener una mayor cantidad de mensajes de depuración en `/var/log/messages` incrementando el valor de la variable `DEBUG`.

`/etc/sysconfig/powersave/events`
: El daemon powersave necesita este archivo para procesar los eventos que se producen en el sistema. A estos eventos se les pueden asignar acciones externas o internas (ejecutadas por el daemon). Con las acciones externas, el daemon intenta activar un archivo ejecutable (normalmente un guión Bash) de `/usr/lib/powersave/scripts/`. Las acciones internas predefinidas son:

  - ignore
  - throttle

- dethrottle
- suspend_to_disk
- suspend_to_ram
- standby
- do_suspend_to_disk
- do_suspend_to_ram
- do_standby
- notify
- screen_saver
- reread_cpu_capabilities

`throttle` limita el procesador en función del valor establecido en `MAX_THROTTLING`. Este valor depende del esquema actual. `dethrottle` hace que el procesador funcione a pleno rendimiento. `suspend_to_disk`, `suspend_to_ram` y `standby` desencadenan eventos de sistema para el modo de reposo. Estas tres acciones son generalmente responsables de activar el modo de reposo, pero siempre deben asociarse a eventos del sistema específicos.

El directorio `/usr/lib/powersave/scripts` contiene guiones para procesar los eventos:

switch_vt
: Es muy útil si la pantalla se muestra distorsionada después de haber estado en reposo o en stand-by.

wm_logout
: Guarda los ajustes y cierra la sesión de GNOME, KDE o de otros gestores de ventanas.

wm_shutdown
: Guarda los ajustes de GNOME o de KDE y apaga el sistema.

set_disk_settings
: Ejecuta los ajustes de disco definidos en `/etc/sysconfig/powersave/disk`.

Por ejemplo, si se define la variable `EVENT_GLOBAL_SUSPEND2DISK="prepare_suspend_to_disk do_suspend_to_disk"`, los dos guiones o acciones se procesarán en el orden especificado en el momento en que el usuario ejecute el comando necesario de powersaved para el modo de reposo, que es `suspend to disk` (Suspender en disco). El daemon inicia el guión externo `/usr/lib/powersave/scripts/prepare_suspend_to_disk` y, una vez que el guión se ha procesado correctamente, el daemon ejecuta la acción interna `do_suspend_to_disk` y pone el equipo definitivamente en modo de reposo después de que el guión haya detenido los servicios y descargado los módulos críticos.

Las acciones para el evento de un botón de reposo (Sleep) se pueden modificar, como en `EVENT_BUTTON_SLEEP="notify suspend_to_disk".` En este caso, se informa al usuario acerca de la suspensión mediante una ventana emergente de X o un mensaje en la consola. A continuación, se genera el evento `EVENT_GLOBAL_SUSPEND2DISK,` que origina las acciones mencionadas y garantiza que el sistema pase al modo de suspensión. La acción interna `notify` se puede personalizar usando la variable `NOTIFY_METHOD` en `/etc/sysconfig/powersave/common.`

`/etc/sysconfig/powersave/cpufreq`
: Incluye variables que permiten optimizar los ajustes de frecuencia de la CPU dinámicos y determinar si se debe usar la implementación del espacio de usuario o del núcleo.

`/etc/sysconfig/powersave/battery`
: En él se definen los límites de las baterías y otros ajustes específicos de la batería.

`/etc/sysconfig/powersave/sleep`
: En este archivo se activan los modos de reposo y se puede definir qué módulos críticos deben descargarse y qué servicios deben detenerse antes de que se produzca un evento de suspensión o de stand-by. Estos módulos se cargarán y los servicios se reiniciarán cuando el sistema se restablezca. Si lo desea, puede incluso retrasar un modo de reposo que se haya iniciado para guardar archivos, por ejemplo. Los ajustes por defecto afectan sobre todo a los módulos USB y PCMCIA. Hay ciertos módulos que pueden provocar fallos en los modos de suspensión o de stand-by.

Consulte la Sección 33.5.4, “Solución de problemas” (p. 641) para obtener más información acerca de la identificación del error.

`/etc/sysconfig/powersave/thermal`
: Activa los controles térmicos y de refrigeración. Puede obtener información adicional sobre este tema en el archivo `/usr/share/doc/packages/powersave/README.thermal`.

`/etc/sysconfig/powersave/disk`
: Este archivo de configuración controla las acciones y los ajustes definidos en relación con el disco duro.

`/etc/sysconfig/powersave/scheme_*`
: Este archivo contiene varios esquemas que regulan el consumo de energía en función de las distintas situaciones de aplicación. Algunos de estos esquemas están ya preconfigurados y pueden utilizarse tal y como están. Aquí también puede almacenar sus propios esquemas personalizados.

33.5.2 Configuración de APM y ACPI

Modos de suspensión y stand-by

Existen tres modos de reposo básicos ACPI y dos APM:

Suspender en disco (ACPI S4, suspensión APM)
: Guarda todo el contenido de la memoria en el disco duro. El equipo se apaga por completo y no consume electricidad. Este modo de reposo está habilitado por defecto y debería funcionar en todos los sistemas.

Suspender en RAM (ACPI S3, suspensión APM)
: Guarda los estados de todos los dispositivos en la memoria principal. Sólo la memoria principal consume electricidad. Este modo de reposo está inhabilitado por defecto porque todavía genera problemas en algunos sistemas. Sin embargo, la compatibilidad se ha ampliado considerablemente.

Stand-by (ACPI S1, stand-by APM)
: Apaga algunos dispositivos (en función del fabricante).

Asegúrese de que las siguientes opciones por defecto estén configuradas en el archivo `/etc/sysconfig/powersave/events` para que sea correcto el procesamiento de los modos de suspensión, stand-by y reanudación (son los ajustes por defecto tras la instalación de SUSE Linux):

```
EVENT_GLOBAL_SUSPEND2DISK=
    "prepare_suspend_to_disk screen_saver do_suspend_to_disk"
EVENT_GLOBAL_SUSPEND2RAM=
    "prepare_suspend_to_ram screen_saver do_suspend_to_ram"
EVENT_GLOBAL_STANDBY=
    "prepare_standby screen_saver do_standby"
EVENT_GLOBAL_RESUME_SUSPEND2DISK=
    "restore_after_suspend_to_disk"
EVENT_GLOBAL_RESUME_SUSPEND2RAM=
    "restore_after_suspend_to_ram"
EVENT_GLOBAL_RESUME_STANDBY=
    "restore_after_standby"
```

Estados personalizados de la batería

En el archivo `/etc/sysconfig/powersave/battery`, puede definir tres estados de carga de la batería (expresados en forma de porcentaje). Cuando se alcanzan dichos estados, el sistema genera alertas o lleva a cabo acciones específicas.

```
BATTERY_WARNING=12
BATTERY_LOW=7
BATTERY_CRITICAL=2
```

En el archivo de configuración `/etc/sysconfig/powersave/events` se definen las acciones o los guiones que han de ejecutarse cuando el nivel de carga es inferior al especificado. En la Sección 33.5.1, “Configuración del paquete powersave” (p. 635) se describe cómo se pueden modificar las acciones por defecto para los botones.

```
EVENT_BATTERY_NORMAL="ignore"
EVENT_BATTERY_WARNING="notify"
EVENT_BATTERY_LOW="notify"
EVENT_BATTERY_CRITICAL="wm_shutdown"
```

Ajuste del consumo de energía en función de las condiciones de trabajo

El rendimiento del sistema se puede adaptar al tipo de suministro de energía. Así, por ejemplo, el consumo de energía del sistema se puede reducir cuando el equipo esté desconectado de la red de suministro eléctrico y funcione con batería. Del mismo modo, el rendimiento se puede aumentar automáticamente en el momento en que el equipo se

conecte de nuevo a la red eléctrica. Para ajustar el consumo, se pueden modificar aspectos como la frecuencia de la CPU, la función de ahorro de energía de IDE y otros parámetros.

En el archivo `/etc/sysconfig/powersave/events` se definen las acciones que se deben ejecutar cuando se conecta el equipo a la red eléctrica o cuando se desconecta de ella. Seleccione los esquemas que se deben usar en `/etc/sysconfig/powersave/common`:

```
AC_SCHEME="performance"
BATTERY_SCHEME="powersave"
```

Los esquemas se almacenan en archivos en `/etc/sysconfig/powersave.` Los nombres de archivo tienen el formato `scheme_nombre-del-esquema.` En el ejemplo, se hace referencia a dos esquemas: `scheme_performance` y `scheme_powersave.` Los esquemas `performance, powersave, presentation` y `acoustic` son esquemas preconfigurados. Los esquemas existentes se pueden editar, crear o suprimir, así como asociarlos a los distintos estados de suministro de energía con la ayuda del módulo de gestión de energía de YaST, que se describe en la Sección 33.6, “Módulo de gestión de energía de YaST” (p. 644).

33.5.3 Funciones ACPI adicionales

Si utiliza ACPI, podrá controlar cómo responde el sistema cuando se usan las *teclas ACPI* (Power, Sleep y las teclas para abrir y cerrar la cubierta). En el archivo `/etc/sysconfig/powersave/events` se establece qué acciones se deben llevar a cabo. Puede obtener información adicional sobre cada una de las opciones en este archivo de configuración.

EVENT_BUTTON_POWER="wm_shutdown"
: Al pulsar la tecla Power, el sistema apaga el gestor de ventanas correspondiente (KDE, GNOME, fvwm, etc.).

EVENT_BUTTON_SLEEP="suspend_to_disk"
: Si pulsa la tecla Sleep, el sistema pasa al modo suspender en disco.

EVENT_BUTTON_LID_OPEN="ignore"
: No pasa nada cuando se abre la cubierta del equipo portátil.

EVENT_BUTTON_LID_CLOSED="screen_saver"
: Cuando se abre la cubierta, se activa el salvapantallas.

EVENT_OTHER="ignore"
: Este evento tiene lugar si el daemon detecta un evento desconocido. Los eventos desconocidos incluyen teclas de activación de ACPI en algunas máquinas.

Si la carga de la CPU no supera un umbral especificado durante un período de tiempo concreto, se puede limitar su potencia. Para ello, especifique un límite de carga en `PROCESSOR_IDLE_LIMIT` y un tiempo de espera en `CPU_IDLE_TIMEOUT`. Si la carga de la CPU se mantiene por debajo del límite durante el tiempo de espera, se activará el evento configurado en `EVENT_PROCESSOR_IDLE`.. Si la CPU vuelve a estar ocupada, se ejecutará `EVENT_PROCESSOR_BUSY`.

33.5.4 Solución de problemas

Todos los mensajes de error y los avisos del sistema se recogen en el archivo `/var/log/messages`. Si no encuentra la información que necesita, aumente el nivel de detalle de los mensajes de powersave usando la opción `DEBUG` del archivo `/etc/sysconfig/powersave/common`. Establezca el valor de la variable en `7` o incluso en `15`, y reinicie el daemon. Cuanto más detallados sean los mensajes de error de `/var/log/messages`, más fácil será identificar los errores. En las siguientes secciones figuran los problemas más habituales que pueden surgir con powersave.

ACPI está activado y es compatible con el hardware pero las funciones no están disponibles

Si surgen problemas con ACPI, use el comando `dmesg|grep -i acpi` para buscar la salida de `dmesg` en los mensajes específicos de ACPI. Para solucionar el error puede ser necesario actualizar el BIOS. Con este fin, visite la página Web del fabricante del equipo portátil, busque una versión actualizada del BIOS e instálela. Informe al fabricante de que debe ajustarse a las especificaciones ACPI más recientes. Si el error persiste después de actualizar el BIOS, proceda de la siguiente forma para sustituir la tabla DSDT defectuosa en el BIOS por una DSDT actualizada:

1. Descargue una DSDT adecuada para el sistema desde `http://acpi.sourceforge.net/dsdt/tables`. Compruebe si el archivo está descomprimido y compilado. Lo reconocerá por la extensión `.aml` (Lenguaje del equipo ACPI, del inglés ACPI Machine Language). Si éste es el caso, continúe con el paso 3.

2 Si la extensión de archivo de la tabla descargada es `.asl` (Lenguaje fuente ACPI, del inglés ACPI Source Language), deberá compilarla con la herramienta iasl (paquete `pmtools`). Ejecute el comando `iasl -sa file.asl`. La versión más reciente de iasl (compilador de ACPI para Intel) está disponible en `http://developer.intel.com/technology/iapc/acpi/downloads.htm`.

3 Copie el archivo `DSDT.aml` donde desee (se recomienda usar `/etc/DSDT.aml`). A continuación, edite `/etc/sysconfig/kernel` y modifique la vía al archivo DSDT en función de los pasos anteriores. Inicie `mkinitrd` (paquete `mkinitrd`). Cuando desinstale el núcleo y use `mkinitrd` para crear `initrd`, la DSDT modificada se integrará y se cargará al arrancar el sistema.

La función de frecuencia de la CPU no funciona

Consulte las fuentes del núcleo (`kernel-source`) para averiguar si el procesador es compatible. Puede que necesite usar un módulo del núcleo o una opción del módulo especiales para activar el control de frecuencia de la CPU. Esta información está disponible en `/usr/src/linux/Documentation/cpu-freq/*`. En caso de que sea necesario emplear un módulo o una opción específicos, configúrelos en el archivo `/etc/sysconfig/powersave/cpufreq` mediante las variables `CPUFREQD_MODULE` y `CPUFREQD_MODULE_OPTS`.

Los modos de suspensión y stand-by no funcionan

Se conocen varios problemas relacionados con el núcleo que pueden ser la causa de que los modos de suspensión y stand-by no funcionen en sistemas ACPI:

- Actualmente, los sistemas con más de 1 GB de RAM no admiten el modo de suspensión.
- Los sistemas con multiprocesador o con un procesador P4 (con tecnología HyperThread) no admiten actualmente el modo de suspensión.

El problema también puede deberse a una implementación defectuosa de la DSDT (BIOS). En este caso, deberá instalar una DSDT nueva.

En sistemas ACPI y APM: cuando el sistema trata de descargar módulos defectuosos, el equipo se bloquea o el evento de suspensión no se activa. También puede ocurrir lo mismo si no se descargan o no se detienen los módulos o los servicios que impiden el

paso al modo de suspensión. En ambos casos, se recomienda localizar el módulo defectuoso que ha impedido que se pase al modo de reposo. Para ello pueden utilizarse los archivos de registro que el daemon powersave genera en `/var/log/suspend2ram.log` y `/var/log/suspend2disk.log`. Si el equipo ni siquiera pasa al modo de reposo, la causa del problema debe buscarse en el módulo descargado en último lugar. Puede manipular los siguientes ajustes del archivo `/etc/sysconfig/powersave/sleep` para descargar los módulos problemáticos antes de pasar a los modos de suspensión o stand-by.

```
UNLOAD_MODULES_BEFORE_SUSPEND2DISK=""
UNLOAD_MODULES_BEFORE_SUSPEND2RAM=""
UNLOAD_MODULES_BEFORE_STANDBY=""
SUSPEND2DISK_RESTART_SERVICES=""
SUSPEND2RAM_RESTART_SERVICES=""
STANDBY_RESTART_SERVICES=""
```

Si se utilizan los modos de suspensión o stand-by en entornos de red cambiantes o con sistemas de archivos montados de forma remota (por ejemplo, Samba o NIS), se recomienda montarlos con automounter o añadir los servicios correspondientes como, por ejemplo, `smbfs` o `nfs,` a las variables mencionadas arriba. En caso de que un programa acceda a un sistema de archivos montado de forma remota antes de iniciarse el modo de suspensión o de stand-by, el servicio no se detendrá correctamente ni el sistema de archivos se desmontará de forma adecuada. Después de restablecer el sistema, puede que el sistema de archivos esté dañado y deba montarse de nuevo.

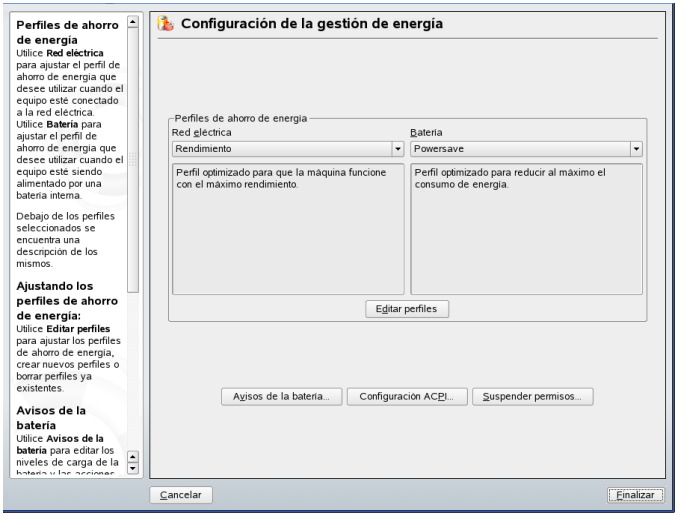
33.5.5 Información adicional

- `/usr/share/doc/packages/powersave`: documentación local del daemon Powersave
- `http://powersave.sourceforge.net`: documentación más reciente del daemon Powersave
- `http://www.opensuse.org/Projects_Powersave`: página de proyecto en el wiki de openSUSE

33.6 Módulo de gestión de energía de YaST

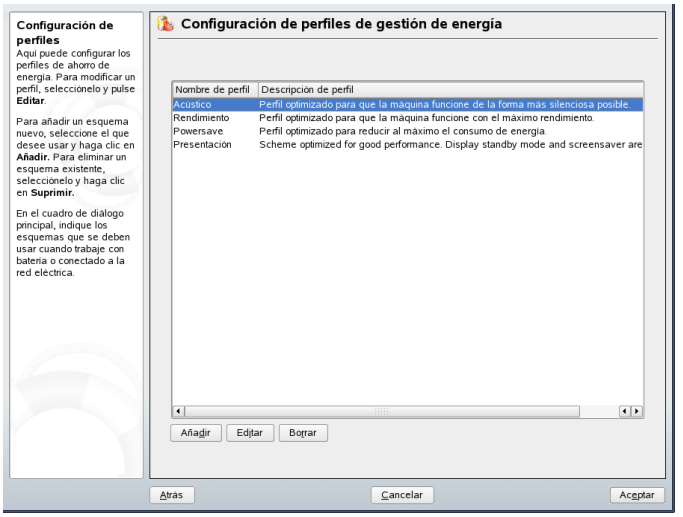
El módulo de gestión de energía de YaST le permite configurar todos los ajustes de gestión de energía descritos en las secciones anteriores. Cuando se inicia el módulo desde el Centro de control de YaST, mediante *Sistema → Gestión de energía,* se muestra el primer cuadro de diálogo del módulo (consulte la Figura 33.1, “Selección de esquemas” (p. 644)).

Figura 33.1 *Selección de esquemas*



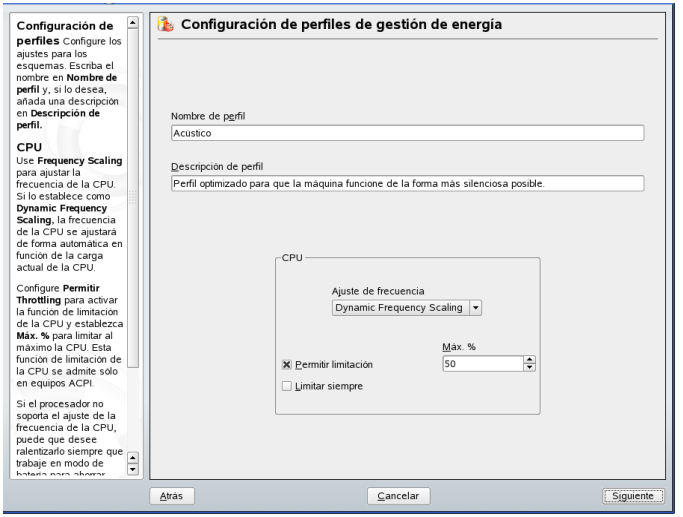
En este cuadro de diálogo, seleccione los esquemas que se deben usar para el funcionamiento con batería y con conexión a la red eléctrica. Para añadir o modificar esquemas, haga clic en *Editar perfiles.* Se abrirá una descripción de los esquemas existentes como la que se muestra en la Figura 33.2, “Descripción general de los esquemas existentes” (p. 645).

Figura 33.2 *Descripción general de los esquemas existentes*



En la descripción general del esquema, seleccione el esquema que desee modificar y haga clic en *Editar.* Para crear un esquema nuevo, haga clic en *Añadir.* El cuadro de diálogo que se abre es igual en ambos casos y es el que se muestra en la Figura 33.3, “Configuración de esquemas” (p. 645).

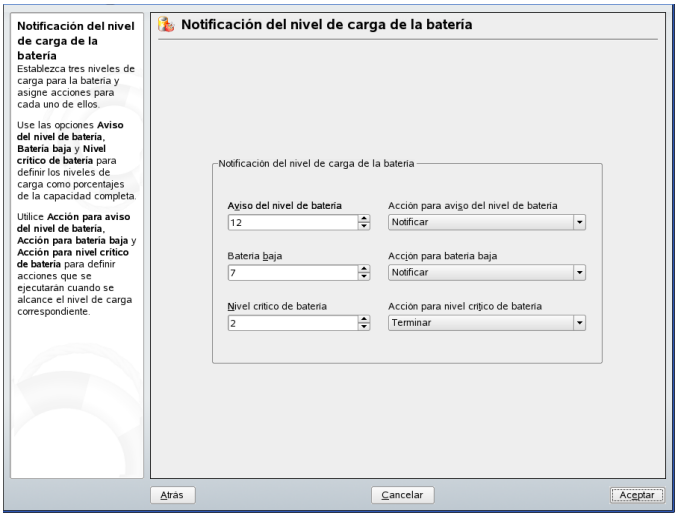
Figura 33.3 *Configuración de esquemas*



En primer lugar, asigne un nombre y una descripción adecuados al perfil que desee crear o modificar. Determine si desea regular el rendimiento de la CPU para este esquema. En caso afirmativo, establezca si se deben usar las funciones de ajuste de la frecuencia y de limitación y cómo se debe hacer. En el siguiente cuadro de diálogo para el disco duro, establezca una directiva para el uso de la función stand-by mediante la opción *Directiva de stand-by* a fin de obtener el máximo rendimiento o para ahorrar la máxima cantidad de energía. Los niveles de ruido del disco duro se pueden ajustar mediante la opción *Directiva acústica* (la admiten pocos discos duros). La opción *Directiva de refrigeración* permite determinar el método de refrigeración que se debe usar. Desafortunadamente, el BIOS sólo admite este tipo de control térmico en raras ocasiones. Consulte `/usr/share/doc/packages/powersave/powersave_manual.html#Thermal` para obtener más información acerca de cómo debe usar el ventilador y los métodos pasivos de refrigeración.

También se pueden efectuar ajustes globales de gestión de energía desde el cuadro de diálogo inicial usando las opciones *Avisos de la batería, Configuración ACPI* o *Activar suspend.* Haga clic en *Avisos de la batería* para acceder al cuadro de diálogo que muestra el nivel de carga de la batería (el que aparece en la Figura 33.4, “Nivel de carga de la batería” (p. 646)).

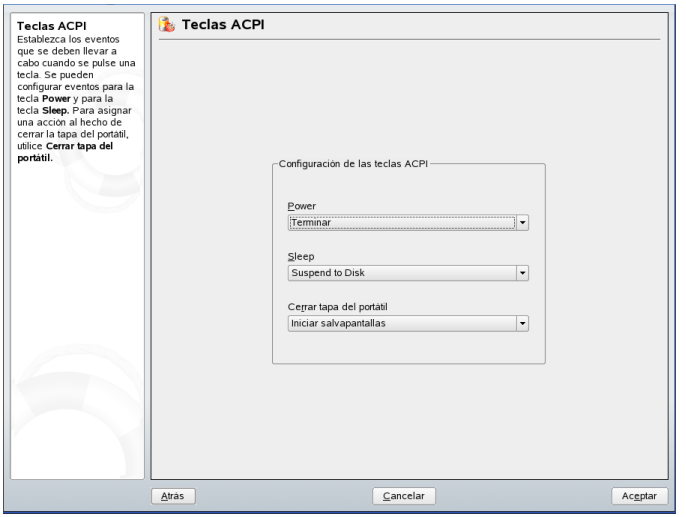
Figura 33.4 *Nivel de carga de la batería*



El BIOS del sistema notifica al sistema operativo si los niveles de carga caen por debajo de ciertos límites que se pueden configurar. En este cuadro de diálogo puede establecer

tres ajustes: *Aviso del nivel de batería, Batería baja* y *Nivel crítico de batería.* Cuando la carga de la batería cae por debajo de estos umbrales, se llevan a cabo acciones específicas. Normalmente, con los dos primeros estados se envía simplemente una nota al usuario. Con el tercero de ellos, se apaga el sistema porque la batería que queda no es suficiente para continuar con el funcionamiento del sistema. Seleccione los niveles de carga adecuados y la acción que se debe realizar. A continuación, haga clic en *Aceptar* para volver al cuadro de diálogo de inicio.

Figura 33.5 *Configuración ACPI*



La opción *Configuración ACPI* se utiliza para acceder al cuadro de diálogo que permite configurar las teclas ACPI. Se muestra en la Figura 33.5, "Configuración ACPI" (p. 647). Los ajustes para las teclas ACPI determinan cómo debe responder el sistema ante ciertos conmutadores; por ejemplo, puede configurar cómo debe responder el sistema cuando se pulsen los botones Power o Sleep o cuando se cierre la cubierta del equipo portátil. Haga clic en *Aceptar* para finalizar la configuración y volver al cuadro de diálogo de inicio.

Haga clic en *Activar suspend* para acceder a un cuadro de diálogo que le permite establecer si los usuarios del sistema pueden usar las funciones de suspensión y stand-by y, en caso afirmativo, cómo deben usarlas. Haga clic en *Aceptar* para volver al cuadro de diálogo principal. Haga clic en *Aceptar* de nuevo para salir del módulo y confirmar los ajustes de gestión de energía.

34 Comunicación inalámbrica

Hay varias maneras de utilizar los sistemas Linux para comunicarse con otros equipos, teléfonos móviles o dispositivos periféricos. Para conectar portátiles en red, se puede utilizar el método WLAN (LAN inalámbrica). Para conectar entre sí componentes de sistema individuales (ratón y teclado), dispositivos periféricos, teléfonos móviles, dispositivos PDA y equipos independientes, se puede utilizar el sistema Bluetooth. IrDA es el más utilizado para establecer comunicación con dispositivos PDA y teléfonos móviles. Este capítulo presenta estas tres tecnologías y su modo de configuración.

34.1 LAN inalámbrica

Las redes de área local (LAN) inalámbricas de han convertido en un aspecto imprescindible de la informática móvil. Hoy en día, la mayoría de portátiles cuentan con tarjetas WLAN integradas. La organización IEEE (Instituto de ingenieros eléctricos y electrónicos) preparó el estándar 802.11 para la comunicación inalámbrica de las tarjetas WLAN. En un principio este estándar ofrecía una velocidad máxima de transmisión de 2 MBit/s. Desde entonces se han añadido varios suplementos para aumentar la velocidad de los datos. En estos suplementos se definen detalles como la modulación, la salida y las velocidades de transmisión:

Tabla 34.1 *Descripción de los distintos estándares de WLAN*

Nombre	Banda (GHz)	Velocidad máxima de transmisión (MBit/s)	Nota
802.11	2,4	2	Obsoleto, ya no queda prácticamente ningún dispositivo final disponible
802.11b	2,4	11	Muy extendido
802,11a	5	54	Menos común
802.11g	2,4	54	Compatibilidad inversa con el 11b

Además, hay estándares patentados como la variación 802.11b de Texas Instruments con una velocidad máxima de transmisión de 22 MBit/s (en ocasiones se hace referencia a ella como 802.11b+). Sin embargo, la popularidad de las tarjetas que usan este estándar es limitada.

34.1.1 Hardware

SUSE Linux no admite las tarjetas 802.11. Sí que son compatibles la mayoría de las tarjetas que usen los estándares 802.11a, 802.11b y 802.11g. Las nuevas tarjetas normalmente cumplen con el estándar 802.11g pero siguen estando disponibles las que usan el 802.11b. Normalmente, se admiten las tarjetas con los chips siguientes:

- Aironet 4500, 4800
- Atheros 5210, 5211, 5212
- Atmel at76c502, at76c503, at76c504, at76c506
- Intel PRO/Wireless 2100, 2200BG, 2915ABG
- Intersil Prism2/2.5/3

- Intersil PrismGT
- Lucent/Agere Hermes
- Ralink RT2400, RT2500
- Texas Instruments ACX100, ACX111
- ZyDAS zd1201

También son compatibles un buen número de tarjetas antiguas que apenas se usan y que ya no están disponibles. Hay disponible una lista exhaustiva de tarjetas WLAN y chips que se usan en el sitio Web de *AbsoluteValue Systems:* `http://www.linux-wlan.org/docs/wlan_adapters.html.gz`. `http://wiki.uni-konstanz.de/wiki/bin/view/Wireless/ListeChipsatz` ofrece una descripción general de los distintos chips de WLAN.

Algunas tarjetas necesitan una imagen de firmware que debe cargarse en la tarjeta donde se ha inicializado el controlador. Este es el caso de Intersil PrismGT, Atmel, TI ACX100 y ACX111. El firmware se puede instalar fácilmente con la actualización en línea de YaST. El firmware para las tarjetas Intel PRO/Wireless está incluido en SUSE Linux y YaST las instala automáticamente tan pronto como se ha detectado una tarjeta de este tipo. Hay disponible más información sobre este asunto en la vía `/usr/share/doc/packages/wireless-tools/README.firmware` del sistema, una vez instalado.

Se pueden usar las tarjetas sin compatibilidad nativa de Linux ejecutando la aplicación ndiswrapper. Ésta utiliza los controladores de Windows XP que vienen con la mayoría de las tarjetas WLAN.

Para configurar ndiswrapper, siga los pasos siguientes:

1. Instale el paquete `ndiswrapper` mediante YaST.
2. Descargue el controlador adecuado de Windows XP correspondiente al adaptador de red inalámbrica. Utilice los controladores mencionados en la lista de tarjetas compatibles en `http://ndiswrapper.sourceforge.net/mediawiki/index.php/List`. Puede que los controladores incluidos en el CD de instalación de la tarjeta de red que no se hayan comprobado funcionen, pero puede que provoquen problemas inesperados.

3 Desempaquete el archivo de reserva. Cada controlador consta de un archivo con la extensión `.inf` y uno o varios archivos DLL. Como usuario Root, instale el controlador con el comando `ndiswrapper -i` *`nombre_controlador`*`.inf`. Se copiarán todos los archivos necesarios en el directorio `/etc/ndiswrapper/` y se crearán los archivos de configuración de la tarjeta.

4 Compruebe si el controlador se ha instalado correctamente con el comando `ndiswrapper -l`.

5 Cargue el módulo con el comando `modprobe ndiswrapper`. El registro del sistema `/var/log/messages` indica si se ha producido un error o se ha instalado correctamente.

6 Si todo va bien, escriba `ndiswrapper -m` para cargar el módulo cuando el sistema se inicie.

7 Configure el adaptador de red inalámbrico en YaST con *Dispositivos de red → Tarjeta de red.* Seleccione *Inalámbrica* en *Tipo de dispositivo,* `0` en *Nombre de la configuración* y `ndiswrapper` para *Nombre del módulo.* Deje los demás campos con sus valores por defecto.

Encontrará una descripción de ndiswrapper en `/usr/share/doc/packages/ndiswrapper/README.SUSE,` una vez instalado el paquete `ndiswrapper.` Para obtener información detallada acerca de ndiswrapper, consulte el sitio Web del proyecto en `http://ndiswrapper.sourceforge.net/support.html`.

34.1.2 Función

En las redes inalámbricas, se usan varias técnicas y configuraciones para asegurar conexiones rápidas, de alta calidad y seguras. Los distintos tipos operativos se adaptan a distintas configuraciones. Puede ser difícil seleccionar el método correcto de autenticación. Los métodos de cifrado disponibles tienen distintas ventajas y riesgos.

Modo operativo

Básicamente, las redes inalámbricas pueden clasificarse como redes gestionadas o ad-hoc. Las redes gestionadas cuentan con un elemento de gestión: el punto de acceso. En este modo (al que también se hace referencia como "modo de infraestructura"), todas

las conexiones de las estaciones WLAN en la red funcionan por el punto de acceso, que también puede servir como conexión a una ethernet. Las redes ad-hoc no cuentan con un punto de acceso. Las estaciones se comunican directamente unas con otras. La velocidad de transmisión y el número de estaciones participantes están muy limitadas en las redes ad-hoc. Por lo tanto, un punto de acceso suele ser más eficaz. Es incluso posible usar una tarjeta WLAN como punto de acceso. La mayoría de tarjetas admiten esta funcionalidad.

Debido a que es más fácil interceptar y poner en peligro una red inalámbrica que una fija, los distintos estándares incluyen métodos de autenticación y de cifrado. En la versión original del estándar IEEE 802.11, se describen con el término WEP. Sin embargo, debido a que WEP ha resultado ser inseguro (consulte “Seguridad” (p. 660)), la industria de WLAN (unida bajo el nombre *Wi-Fi Alliance*) ha definido una nueva extensión denominada "WPA" que debería eliminar los puntos vulnerables de WEP. El estándar posterior IEEE 802.11i (también conocido como "WPA2" debido a que WPA está basado en la versión no final de 802.11i) incluye WPA y algunos otros métodos de autenticación y cifrado.

Autenticación

Para garantizar que sólo se puedan conectar las estaciones autorizadas, en las redes gestionadas se usan varios mecanismos de autenticación:

Abrir
: Un sistema abierto es un sistema que no requiere autenticación. Cualquier estación puede unirse a la red. No obstante, se puede usar el cifrado WEP (consulte “Cifrado” (p. 655)).

Clave compartida (según el estándar IEEE 802.11)
: En este procedimiento, se usa la clave WEP para la autenticación. Sin embargo, no se recomienda este procedimiento porque la clave WEP es más propensa a recibir ataques. Todo lo que necesita hacer un atacante es escuchar el tiempo suficiente la comunicación entre la estación y el punto de acceso. Durante el proceso de autenticación, ambos lados intercambian la misma información, una vez de manera cifrada y otra no cifrada. Esto hace posible que la clave se reconstruya con herramientas adecuadas. Puesto que este método hace uso de la clave WEP para la autenticación y el cifrado, no mejora la seguridad de la red. Una estación que tiene la clave WEP correcta puede autenticar, cifrar y descifrar. Una estación que no cuenta con la clave correcta no puede descifrar los paquetes recibidos. De la misma

forma, no puede comunicarse, sin tener en cuenta si tuvo que autenticarse a sí misma.

WPA-PSK (según el estándar IEEE 802.1x)
: WPA-PSK (PSK significa "preshared key", clave compartida previamente) funciona de manera parecida al procedimiento de clave compartida. Todas las estaciones participantes y el punto de acceso necesitan la misma clave. La clave tiene 256 bits de longitud y normalmente se introduce como una contraseña. Este sistema no necesita una gestión compleja de claves como WPA-EAP y es más adecuado para uso privado. Por tanto, en ocasiones se hace referencia a WPA-PSK como “Home”.

WPA-EAP (según el estándar IEEE 802.1x)
: En realidad, WPA-EAP no es un sistema de autenticación sino un protocolo para transportar información de autenticación. WPA-EAP se utiliza para proteger redes inalámbricas en empresas. En redes privadas, apenas se usa. Por esta razón, a veces se hace referencia a WPA-EAP como WPA “Enterprise”.

  WPA-EAP necesita un servidor Radius para autenticar usuarios. EAP ofrece tres métodos distintos de conectar y autenticar con el servidor: TLS (Seguridad de nivel de transporte), TTLS (Seguridad de nivel de transporte con forma de túnel) y PEAP (Protocolo de autenticación extensible protegida). En pocas palabras, estas opciones funcionan de la siguiente forma:

  EAP-TLS
  : La autenticación TLS se basa en el intercambio mutuo de certificados tanto para el servidor como para el cliente. En primer lugar, el servidor presenta este certificado al cliente donde se evalúa. Si el certificado se considera válido, el cliente presenta su certificado al servidor. Aunque TLS es seguro, necesita una infraestructura de gestión de certificación en funcionamiento en la red. Esta infraestructura apenas se encuentra en redes privadas.

  EAP-TTLS y PEAP
  : Tanto TTLS como PEAP son protocolos de dos fases. En la primera, se establece un modo seguro y en la segunda se intercambian los datos de autenticación del cliente. Necesitan mucho menos sobrecargo de gestión de certificación que TLS (o ninguno en absoluto).

Cifrado

Existen varios métodos de cifrado para asegurar que ninguna persona sin autorización pueda leer los paquetes de datos que se intercambian en una red inalámbrica o tenga acceso a la red:

WEP (definido en IEEE 802.11)
: Este estándar hace uso del algoritmo de cifrado RC4, con una longitud de clave original de 40 bits, posteriormente con 104 bits. Con frecuencia, la longitud es de 64 bits o 128 bits, dependiendo de si se incluyen los 24 bits del vector de inicialización. Sin embargo, este estándar tiene algunos puntos débiles. Los ataques contra las claves generadas por este sistema pueden tener éxito. No obstante, es mejor usar WEP que no cifrar en absoluto la red.

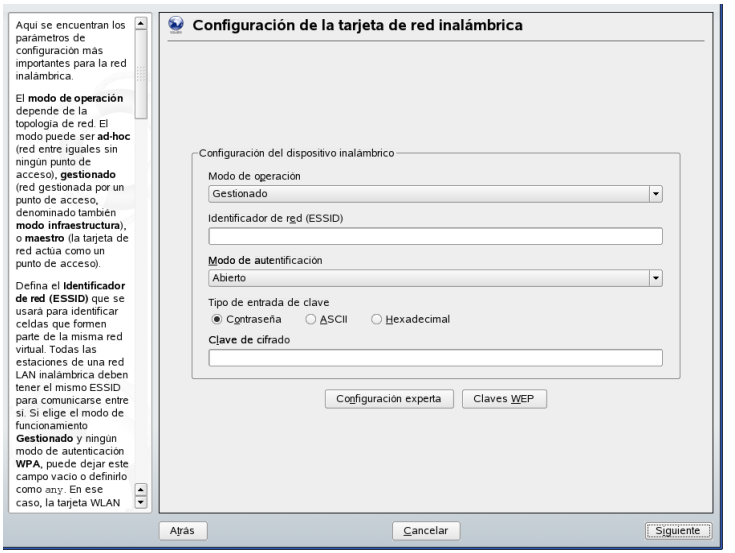
TKIP (definido en WPA/IEEE 802.11i)
: Este protocolo de gestión de claves definido en el estándar WPA emplea el mismo algoritmo de cifrado que WEP pero elimina su debilidad. Debido a que se genera una nueva clave para cada paquete de datos, los ataques contra estas claves son infructuosos. TKIP se usa junto con WPA-PSK.

CCMP (definido en IEEE 802.11i)
: CCMP describe la gestión de claves. Normalmente se usa en conexión con WPA-EAP, pero también se puede usar con WPA-PSK. El cifrado tiene lugar según AES y es más fuerte que el cifrado RC4 del estándar WEP.

34.1.3 Configuración con YaST

Para configurar la tarjeta de red inalámbrica, inicie el módulo *Tarjeta de red* de YaST. También puede seleccionar si desea usar YaST o NetworkManager para gestionar la tarjeta de red. Si selecciona YaST, elija el tipo de dispositivo *Inalámbrica* en *Configuración de la dirección de red* y haga clic en *Siguiente*. En *Configuración de la tarjeta de red inalámbrica* que aparece en la Figura 34.1, “YaST: configuración de la tarjeta de red inalámbrica” (p. 656), realice los ajustes básicos para la operación WLAN:

Figura 34.1 *YaST: configuración de la tarjeta de red inalámbrica*



Modo operativo
: Las estaciones pueden integrarse en una WLAN de tres modos distintos. El modo adecuado depende de la red en la que comunicar: *Ad-hoc* (red par a par sin punto de acceso), *Gestionado* (la red está gestionada por un punto de acceso) o *Maestro* (la tarjeta de red debería usarse como el punto de acceso). Para usar cualquiera de los modos WPA-PSK o WPA-EAP, el modo operativo debe definirse en *Gestionado.*

Nombre de la red (ESSID)
: Todas las estaciones de una red inalámbrica necesitan el mismo ESSID para comunicarse entre ellas. Si no se especifica nada, la tarjeta seleccionará automáticamente un punto de acceso que puede no ser el deseado.

Modo de autenticación
: Seleccione un método de autenticación adecuado para la red: *Abierto, Clave compartida, WPA-PSK* o *WPA-EAP.* Si selecciona la autenticación WPA, deberá definir un nombre de red.

Configuración avanzada
: Este botón abre un cuadro de diálogo para la configuración detallada de la conexión WLAN. Más adelante se ofrecerá una descripción detallada de este cuadro de diálogo.

Después de completar los ajustes básicos, la estación estará lista para su implantación en la WLAN.

IMPORTANTE: Seguridad en redes inalámbricas

Asegúrese de usar los métodos de cifrado y autenticación compatibles para proteger el tráfico de la red. Las conexiones WLAN sin cifrar permiten que terceros intercepten todos los datos de la red. Un cifrado débil (WEP) es mejor que no tener ninguno. Consulte "Cifrado" (p. 655) y "Seguridad" (p. 660) para obtener información.

Según el método de autenticación seleccionado, YaST le pedirá que defina los ajustes en otro cuadro de diálogo. En el caso de *Abierto* no hay nada que configurar porque este ajuste implanta la operación no cifrada sin autenticación.

Claves WEP

Defina un tipo de clave de entrada. Elija entre *Contraseña, ASCII* o *Hexadecimal.* Puede mantener hasta cuatro claves distintas para cifrar los datos transmitidos. Haga clic en *Claves múltiples* para entrar en el cuadro de diálogo de configuración. Defina la longitud de la clave: *128 bits* o *64 bits.* El ajuste por defecto es *128 bits.* En el área de la lista situada en la parte inferior del cuadro de diálogo, se pueden especificar hasta cuatro claves distintas que la estación usará para cifrar. Pulse *Definir como predeterminada* para definir una de ellas como la clave por defecto. A menos que lo cambie, YaST usará la primera clave introducida como la clave por defecto. Si se suprime la clave estándar, una de las otras claves deberá marcarse manualmente como la clave por defecto. Haga clic en *Editar* para modificar las entradas de la lista existentes o crear nuevas claves. En este caso, una ventana emergente le pedirá que seleccione un tipo de entrada (*Contraseña, ASCII* o *Hexadecimal*). Si selecciona *Contraseña,* escriba una palabra o cadena de caracteres a partir de la cual se generará una clave de acuerdo con la longitud previamente especificada. *ASCII* necesita una entrada de 5 caracteres para una clave de 64 bits y 13 caracteres para una de 128 bits. En el caso de *Hexadecimal* introduzca 10 caracteres para una clave de 64 bits o 26 caracteres para una de 128 bits en notación hexadecimal.

WPA-PSK

Para introducir una clave para WPA-PSK, seleccione el método de entrada: *Contraseña* o *Hexadecimal.* En el modo *Contraseña* la entrada debe tener de 8 a 63 caracteres. En el modo *Hexadecimal* introduzca 64 caracteres.

WPA-EAP
: Introduzca las credenciales que el administrador de red le haya proporcionado. En el caso de TLS, introduzca el *certificado de cliente* y el *certificado de servidor.* TTLS y PEAP necesitan la *identidad* y la *contraseña.* El *certificado de servidor* es opcional. YaST busca cualquier certificado en `/etc/cert` así que guarde los certificados que reciba en esa ubicación y restrinja el acceso a estos archivos a `0600` (derechos de lectura y escritura del propietario).

  Haga clic en *Configuración avanzada* para acceder al cuadro de diálogo de autenticación avanzada para la configuración de WPA-EAP. Seleccione el método de autenticación para la segunda fase de la comunicación EAP-TTLS o EAP-PEAP. Si ha seleccionado TTLS en el cuadro de diálogo previo, seleccione `auto, MD5, GTC, CHAP, PAP, MSCHAPv1` o `MSCHAPv2.` Si ha seleccionado PEAP, seleccione `auto, MD5, GTC` o `MSCHAPv2.` Se puede usar la *versión de PEAP* para forzar el uso de una implementación de PEAP concreta si el ajuste que se ha determinado automáticamente no funciona. Salga de este cuadro de diálogo haciendo clic en *Aceptar.*

Haga clic en *Configuración avanzada* para abandonar el cuadro de diálogo de la configuración básica de la conexión WLAN e introducir la configuración avanzada. Las siguientes opciones están disponibles en este cuadro de diálogo:

Canal
: La especificación de un canal en el que la estación WLAN debería trabajar sólo es necesaria en los modos *Ad-hoc* y *Maestro.* En el modo *Gestionado,* la tarjeta busca automáticamente los canales disponibles para los puntos de acceso. En el modo *Ad-hoc* seleccione uno de los 12 canales que se ofrecen para la comunicación de la estación con las demás. En el modo *Maestro,* determine el canal en el que la tarjeta debería ofrecer funciones de punto de acceso. El ajuste por defecto para esta opción es *Auto.*

Tasa de bits
: Según el rendimiento de la red, puede querer definir una tasa de bits para la transmisión de un punto a otro. En el ajuste por defecto *Auto,* el sistema intentará usar la tasa de transmisión de datos más alta posible. Algunas tarjetas WLAN no admiten este ajuste de tasa de bits.

Puntos de acceso
: En un entorno con varios puntos de acceso, puede seleccionarse uno de ellos previamente especificando la dirección MAC.

Usar gestión de energía
: Cuando está viajando, utilice las tecnologías de ahorro de energía para maximizar el tiempo de funcionamiento de la batería. Hay más información disponible sobre la gestión de energía en el Capítulo 33, *Gestión de energía* (p. 621).

34.1.4 Utilidades

hostap (paquete `hostap`) se usa para ejecutar una tarjeta WLAN como un punto de acceso. Hay más información disponible sobre este paquete en la página de principal del proyecto (`http://hostap.epitest.fi/`).

kismet (paquete `kismet`) es una herramienta de diagnóstico de red con la que escuchar el tráfico de paquetes de WLAN. De esta forma, también puede detectar cualquier intento de intrusión en la red. Hay más información disponible en `http://www.kismetwireless.net/` y en la lista concisa de comandos.

34.1.5 Sugerencias y consejos prácticos para configurar una WLAN

Estos consejos le ayudarán a conseguir más velocidad y estabilidad además de mejorar algunos aspectos de seguridad de la WLAN.

Estabilidad y velocidad

El rendimiento y fiabilidad de una red inalámbrica depende principalmente de si las estaciones participantes reciben una señal limpia de las otras estaciones. Los obstáculos como los cortafuegos contribuyen a debilitar la señal. Cuanto más disminuye la fuerza de la señal, más se ralentiza la transmisión. Durante la operación, compruebe la fuerza de la señal con la utilidad iwconfig en la línea de comando (campo `Calidad del enlace`) o con KInternet en KDE. Si tiene problemas con la calidad de la señal, pruebe a configurar los dispositivos en otro lugar o a ajustar la posición de las antenas de los puntos de acceso. Hay antenas auxiliares que mejoran en gran medida la recepción para muchas tarjetas PCMCIA WLAN. La tasa especificada por el fabricante, como 54 MBit/s, es un valor nominal que representa la velocidad máxima teórica. En la práctica, el rendimiento máximo de los datos no es superior a la mitad de este valor.

Seguridad

Si desea configurar una red inalámbrica, recuerde que cualquier persona dentro de su rango de transmisión puede acceder fácilmente si no se implantan medidas de seguridad. Por tanto, asegúrese de activar un método de cifrado. Todas las tarjetas WLAN y los puntos de acceso admiten el cifrado WEP. Aunque no es completamente seguro, presenta un obstáculo a un atacante potencial. WEP normalmente es suficiente para el uso privado. WPA-PSK sería incluso mejor pero no está implantado en puntos de acceso más antiguos o routers con funciones de WLAN. En algunos dispositivos, puede implantarse WPA mediante una actualización de firmware. Además, Linux no admite WPA en todos los componentes de hardware. En el momento de la redacción de este documento, WPA sólo funcionaba con tarjetas que usaban chips Atheros, Intel PRO/Wireless o Prism2/2.5/3. En el caso de Prism2/2.5/3, WPA sólo funciona si se utiliza el controlador de hostap (consulte “Problemas con las tarjetas Prism2” (p. 660)). Si WPA no está disponible, WEP es mejor que no usar ningún cifrado. En empresas con requisitos avanzados de seguridad, las redes inalámbricas sólo deberían funcionar con WPA.

34.1.6 Solución de problemas

Si la tarjeta WLAN no responde, compruebe si ha descargado el firmware necesario. Consulte la Sección 34.1.1, “Hardware” (p. 650). Los párrafos que vienen a continuación explican algunos problemas conocidos.

Varios dispositivos de red

Los portátiles modernos normalmente tienen una tarjeta de red y una WLAN. Si ha configurado ambos dispositivos con DHCP (asignación automática de direcciones), es posible que tenga problemas con la resolución de nombres y el gateway por defecto. Este problema es fácilmente identificable porque puede hacer ping en el router pero no puede navegar por Internet. La base de datos de asistencia técnica en `http://portal.suse.com` cuenta con un artículo sobre este asunto. Para encontrar el artículo, introduzca “DHCP” en el cuadro de diálogo de búsqueda.

Problemas con las tarjetas Prism2

Hay varios controladores disponibles para dispositivos con chips Prism2. Esas tarjetas funcionan relativamente bien con los distintos controladores. Con estas tarjetas, sólo

es posible usar WPA con el controlador hostap. Si una de esas tarjetas no funciona correctamente, no funciona en absoluto o desea usar WPA, lea `/usr/share/doc/packages/wireless-tools/README.prism2`.

WPA

La compatibilidad de WPA es bastante reciente en SUSE Linux y todavía está en fase de desarrollo. Por tanto, YaST no admite la configuración de todos los modos de autenticación de WPA. No todas las tarjetas LAN inalámbricas y controladores admiten WPA. Algunas tarjetas necesitan una actualización de firmware para habilitar WPA. Si desea usar WPA, lea `/usr/share/doc/packages/wireless-tools/README.wpa`.

34.1.7 Información adicional

Las páginas de Internet de Jean Tourrilhes, desarrollador de las *herramientas inalámbricas* para Linux, contienen información muy útil y valiosa sobre redes inalámbricas. Consulte `http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html`.

34.2 Bluetooth

Bluetooth es una tecnología inalámbrica que permite conectar varios dispositivos, como teléfonos móviles, PDA, dispositivos periféricos o componentes del sistema, como el teclado o el ratón. El nombre tiene su origen en el rey danés Harold Bluetooth, que logró unir varias facciones enfrentadas de la región escandinava. El logotipo de Bluetooth se basa en las runas de sus iniciales “H” (parecido a una estrella) y “B.”

Bluetooth se diferencia de IrDA en algunos aspectos importantes: por una parte, los dispositivos no necesitan “verse” el uno al otro directamente y, por otra, varios dispositivos pueden agruparse y formar redes completas. No obstante, la transferencia máxima de datos es de 720 Kbps (en la versión actual, que es la 1.2). En teoría, con Bluetooth se pueden establecer conexiones entre dispositivos separados por una pared. En la práctica, sin embargo, esto depende del tipo de pared y de la clase de dispositivos. Existen tres clases de dispositivos con alcances de transmisión de entre 10 y 100 metros.

34.2.1 Fundamentos

En las siguientes secciones se describen los principios básicos del funcionamiento de Bluetooth. Conozca qué requisitos de software se deben cumplir, cómo interactúa Bluetooth con su sistema y cómo configura Bluetooth el trabajo mediante perfiles.

Software

Para poder utilizar Bluetooth es necesario contar con un adaptador Bluetooth (integrado en el dispositivo o bien un dispositivo externo), controladores y el stack de protocolo para Bluetooth. El núcleo de Linux contiene ya los controladores básicos para usar Bluetooth. En cuanto al stack de protocolo, se utiliza el sistema Bluez. Para asegurarse de que las aplicaciones funcionan con Bluetooth, es necesario instalar los paquetes básicos `bluez-libs` y `bluez-utils`. Dichos paquetes proporcionan servicios y utilidades que el sistema necesita. Además, para algunos adaptadores como Broadcom o AVM BlueFritz!, se requiere también el paquete `bluez-firmware`. El paquete `bluez-cups` permite imprimir a través de conexiones Bluetooth. Si tiene que depurar problemas relacionados con las conexiones Bluetooth, instale el paquete `bluez-hcidump`.

Interacción general

Los sistemas Bluetooth están formados por cuatro capas interdependientes, cada una de las cuales cumple una función determinada:

Hardware
: El adaptador y un controlador adecuado que garantiza la compatibilidad con el núcleo de Linux.

Archivos de configuración
: Se utilizan para controlar el sistema Bluetooth.

Daemons
: Servicios que proporcionan diversas funciones y que están controlados a través de los archivos de configuración.

Aplicaciones
: Programas que ponen al alcance del usuario las funciones proporcionadas por los daemons y que les permiten controlar dichas funciones.

Al conectar un adaptador Bluetooth, el controlador correspondiente se carga a través del sistema HotPlug. Una vez que el controlador está cargado, se comprueba por medio de los archivos de configuración si Bluetooth debe iniciarse. En caso afirmativo, se determina qué servicios deben iniciarse y, dependiendo de estos datos, se activan los daemons correspondientes. Los adaptadores de Bluetooth se prueban en la instalación. Si se encuentran uno o varios, Bluetooth se activa. De lo contrario, el sistema Bluetooth se desactiva. Los dispositivos Bluetooth que se añadan posteriormente deberán habilitarse de forma manual.

Perfiles

Los servicios en Bluetooth se definen por medio de perfiles como, por ejemplo, el perfil de transferencia de archivos, el perfil de impresión básica y el perfil de red de área personal. Para que un dispositivo pueda utilizar un servicio de otro, ambos deben entender el mismo perfil. Desafortunadamente, ni el manual ni la caja del dispositivo suelen incluir esta información. Otro problema es que algunos fabricantes respetan escrupulosamente la definición de los perfiles individuales, pero otros no. A pesar de todo esto, las comunicaciones entre los dispositivos suelen funcionar sin problema.

En el siguiente texto, los dispositivos locales son los que están conectados físicamente al equipo. Los demás dispositivos que sólo pueden acceder mediante conexiones inalámbricas reciben el nombre de "dispositivos remotos".

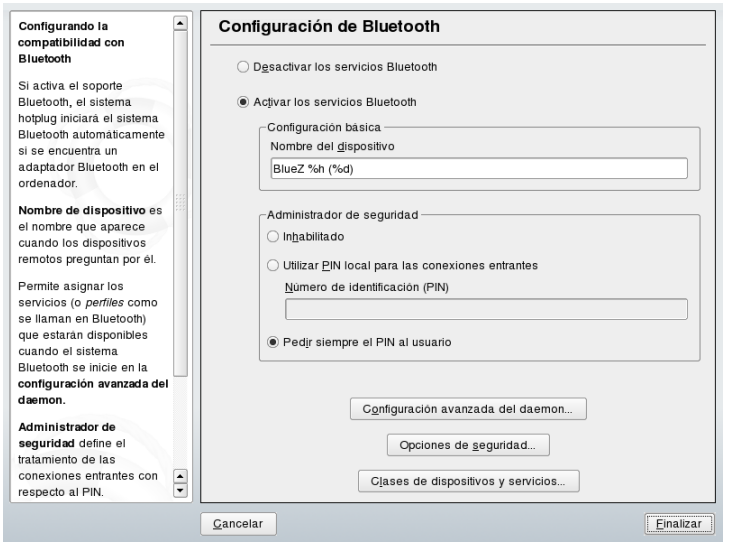
34.2.2 Configuración

En esta sección se presenta la configuración de Bluetooth. Conozca qué archivos de configuración participan, qué herramientas se necesitan y cómo se configura Bluetooth con YaST o de forma manual.

Configuración de Bluetooth con YaST

El módulo Bluetooth de YaST (que se muestra en la Figura 34.2, “Configuración de Bluetooth con YaST” (p. 664)) le permite configurar la compatibilidad de Bluetooth con su sistema. En el momento en que HotPlug detecta un adaptador Bluetooth en el sistema (por ejemplo, durante el arranque o cuando se conecta un adaptador), Bluetooth se inicia automáticamente con los ajustes establecidos en este módulo.

Figura 34.2 *Configuración de Bluetooth con YaST*



En el primer paso de la configuración, debe determinar si los servicios Bluetooth tienen que iniciarse en el sistema. Si ha habilitado los servicios de Bluetooth, hay dos cosas que se pueden configurar. En primer lugar, el *Nombre del dispositivo.* Éste es el nombre que muestran otros dispositivos cuando se detecta su equipo. Hay dos marcadores de posición disponibles: `%h` hace referencia al nombre de host del sistema (es útil, por ejemplo, si se usa una asignación dinámica mediante DHCP) y `%d,` que inserta el número de interfaz (es útil sólo si dispone de más de un adaptador Bluetooth en el equipo). Por ejemplo, si escribe `Portátil %h` en el campo y DHCP asigna el nombre `unit123` al equipo, los demás dispositivos remotos verán su equipo con el nombre `Portátil unit123.`

El parámetro *Administrador de seguridad* está relacionado con el comportamiento del sistema local cuando un dispositivo remoto intenta conectarse. La diferencia radica en la gestión que se hace del número PIN. Se puede establecer que cualquier dispositivo pueda conectarse sin usar un PIN o se puede determinar cómo se elige el PIN correcto en caso de que se necesite uno. Puede especificar un PIN (almacenado en un archivo de configuración) en el campo de entrada pertinente. Si un dispositivo intenta conectarse, usará en primer lugar este PIN. Si falla, intentará conectarse sin PIN. Para obtener la mayor seguridad, se aconseja elegir *Pedir siempre el PIN al usuario.* Esta opción permite usar diferentes PIN para los distintos dispositivos remotos.

Haga clic en *Configuración avanzada del daemon* para acceder al cuadro de diálogo con objeto de seleccionar y configurar los servicios disponibles (llamados *perfiles* en Bluetooth). Se muestra una lista de todos los servicios disponibles, los cuales puede activar o desactivar con los botones de activación o desactivación. Haga clic en *Editar* para abrir un cuadro de diálogo en el que podrá especificar argumentos adicionales para el servicio seleccionado (daemon). No haga ningún cambio, a menos que esté familiarizado con el servicio. Después de configurar el daemon, salga de este cuadro de diálogo haciendo clic en *Aceptar.*

En el cuadro de diálogo principal, haga clic en *Opciones de seguridad* para acceder al cuadro de diálogo de seguridad con objeto de especificar las opciones de cifrado, autenticación y exploración. A continuación, salga del cuadro de diálogo de seguridad para volver al principal. Cuando cierre el cuadro de diálogo principal con la opción *Finalizar,* el sistema Bluetooth estará listo para su uso.

Desde el cuadro de diálogo principal, puede acceder también al cuadro de diálogo *Clases de dispositivos y servicios.* Los dispositivos Bluetooth se agrupan en distintas clases de dispositivos. En este cuadro de diálogo, elija la clase adecuada para su equipo como, por ejemplo, *Escritorio* o *Portátil.* La clase de dispositivo no es muy relevante, a diferencia de las clases de servicios, que también se configuran aquí. En ocasiones, los dispositivos Bluetooth remotos como, por ejemplo, los teléfonos móviles, sólo permiten ciertas funciones si pueden detectar la clase de servicios adecuada establecida en el sistema. Suele ser el caso de los teléfonos móviles que esperan una clase llamada *Transferencia de objetos* antes de permitir la transferencia de archivos con el equipo. Puede elegir varias clases, aunque no es eficaz seleccionarlas todas sólo "por si acaso". La selección por defecto suele ser adecuada en la mayoría de los casos.

Para usar Bluetooth para configurar una red, active *PAND* en el cuadro de diálogo *Configuración avanzada del daemon* y defina el modo del daemon con *Editar.* Para que la conexión de red Bluetooth funcione, pand debe operar en el modo de escucha y el par en el modo de búsqueda. El modo por defecto es el de escucha. Si es necesario, ajuste el modo del pand local. Además, configure le interfaz `bnepX` (`X` hace referencia al número de dispositivo en el sistema) en el módulo *Tarjeta de red* de YaST.

Configuración manual de Bluetooth

Los archivos de configuración para los distintos componentes del sistema Bluez se encuentran en el directorio `/etc/bluetooth`. La única excepción es el archivo `/etc/sysconfig/bluetooth` para iniciar los componentes, y que se modifica mediante el módulo YaST.

Los archivos de configuración que se describen a continuación sólo puede modificarlos el usuario `Root`. Actualmente no hay ninguna interfaz gráfica que permita cambiar todos los ajustes, aunque los más importantes se pueden definir usando el módulo Bluetooth de YaST, que se describe en "Configuración de Bluetooth con YaST" (p. 663). Los demás ajustes sólo deben modificarlos los usuarios experimentados en circunstancias especiales. No obstante, los ajustes por defecto suelen ser adecuados.

Un número PIN proporciona una protección básica frente a conexiones no deseadas. Los teléfonos móviles suelen pedir este número PIN cuando establecen el primer contacto (o al configurar un contacto de dispositivo en el teléfono). Para que dos dispositivos puedan comunicarse entre sí, ambos deben identificarse con el mismo PIN. En el equipo, el número PIN se encuentra en el archivo `/etc/bluetooth/pin`.

IMPORTANTE: Seguridad en las conexiones Bluetooth

El uso de números PIN no garantiza que la transmisión entre dos dispositivos sea totalmente segura. Tenga en cuenta que tanto la autenticación como el cifrado de las conexiones Bluetooth están desactivados por defecto. La activación de la autenticación y del cifrado puede provocar problemas de comunicación con algunos dispositivos Bluetooth.

En el archivo de configuración `/etc/bluetooth/hcid.conf` se pueden modificar varios ajustes, tales como los nombres de dispositivos y el modo de seguridad. No obstante, los ajustes por defecto suelen ser adecuados. El archivo incluye comentarios que describen las opciones de los distintos ajustes.

En el archivo se incluyen dos secciones, una de ellas dedicada a las opciones y otra a los dispositivos. La primera contiene información general que usa hcid para el inicio. La segunda sección incluye ajustes para cada dispositivo Bluetooth local.

Uno de los ajustes más importantes de la sección de opciones es `security auto;` (Seguridad automática). Si se configura en `auto` (Automática), hcid intentará usar el PIN local para las conexiones entrantes. Si se produce un fallo, cambiará a `none` (Ninguno) y se establecerá la conexión de todos modos. Para obtener una mayor seguridad, este ajuste por defecto debe establecerse en `user` (Usuario) con objeto de asegurarse de que se solicite un número PIN al usuario cada vez que se establezca una conexión.

En la sección de dispositivos puede especificar el nombre con el que se mostrará el equipo en el otro extremo de la conexión. En esta sección se define la clase de dispositivo

como, por ejemplo, `Desktop` (Escritorio), `Laptop` (Portátil) o `Server` (Servidor). La autenticación y el cifrado también se habilitan o inhabilitan desde aquí.

34.2.3 Utilidades y componentes del sistema

El uso de Bluetooth depende de la interacción de varios servicios. Como mínimo, es necesario que se estén ejecutando dos daemons en segundo plano: hcid (daemon de la interfaz del controlador del host), que actúa como interfaz del dispositivo Bluetooth y lo controla; y sdpd (daemon del protocolo de descubrimiento de servicios), mediante el cual un dispositivo puede averiguar qué servicios ofrece el host. Si no se activan automáticamente al iniciar el sistema, tanto hcid como sdpd puede activarse con el comando `rcbluetooth start.` Este comando se debe ejecutar como usuario `Root.`

A continuación, se describen las principales herramientas de shell que se pueden usar para trabajar con Bluetooth. Aunque ya existen diversos componentes gráficos para manejar Bluetooth, merece la pena conocer estos programas.

Algunos de estos comandos sólo se pueden ejecutar como usuario `Root,` por ejemplo, el comando `l2ping` *`device_address,`* con el que puede probar la conexión a un dispositivo remoto.

hcitool

Mediante hcitool es posible averiguar si se han encontrado dispositivos locales y remotos. El comando `hcitool dev` muestra una lista de los dispositivos locales. La salida genera una línea con el formato *`nombre_interfaz dirección_dispositivo`* para cada dispositivo local detectado.

Para detectar dispositivos remotos, puede utilizarse el comando `hcitool inq.` Se devuelven tres valores para cada dispositivo detectado: la dirección del dispositivo, la diferencia horaria y la clase de dispositivo. La dirección del dispositivo es importante porque los otros comandos la usan para identificar el dispositivo de destino. La diferencia horaria se usa fundamentalmente para propósitos técnicos. La clase hace referencia al tipo de dispositivo y de servicio como un valor hexadecimal.

El comando `hcitool name` *`dirección_dispositivo`* se puede usar para determinar el nombre de un dispositivo remoto. Si se trata de un equipo remoto, la clase y el nombre de dispositivo deben coincidir con la información que figura en `/etc/`

`bluetooth/hcid.conf`. Las direcciones de los dispositivos locales generan un error.

hciconfig

El comando `/usr/sbin/hciconfig` proporciona información adicional sobre el dispositivo local. Si `hciconfig` se ejecuta sin argumentos, la salida mostrará la información del dispositivo como, por ejemplo, el nombre del dispositivo (`hciX`), la dirección del dispositivo físico (un número de 12 dígitos con el formato `00:12:34:56:78`), así como información acerca de la cantidad de datos transmitidos.

`hciconfig hci0 name` muestra el nombre que devuelve el equipo cuando recibe peticiones desde dispositivos remotos. El comando `hciconfig` no sólo sirve para ver los ajustes del dispositivo local, sino también para modificarlos. Por ejemplo, el comando `hciconfig hci0 name PRUEBA` asigna al dispositivo el nombre `PRUEBA`.

sdptool

El programa sdptool se puede usar para comprobar qué servicios ofrece un dispositivo específico. El comando `sdptool browse` *`dirección_dispositivo`* muestra todos los servicios de un dispositivo, mientras que `sdptool search` *`código_servicio`* permite buscar un servicio concreto. Este comando analiza todos los servicios accesibles para el servicio solicitado. Si uno de los dispositivos ofrece el servicio, el programa imprime el nombre completo del servicio devuelto por el dispositivo junto con una breve descripción. Al ejecutar `sdptool` sin ningún parámetro, se muestra una lista con todos los códigos de servicio posibles.

34.2.4 Aplicaciones gráficas

En Konqueror, escriba la dirección URL `bluetooth:/` para que se muestren los dispositivos Bluetooth locales y remotos. Haga doble clic en un dispositivo para ver una descripción de los servicios ofrecidos por el dispositivo. Si se desplaza con el ratón por los distintos servicios especificados, en la barra de estado del navegador se mostrará qué perfil está usando el servicio. Si hace clic en un servicio, se abrirá un cuadro de diálogo donde debe indicar la acción que desea realizar: guardar, usar el servicio (para ello deberá iniciarse una aplicación) o cancelar la acción. Marque una casilla de verificación si no desea que se muestre de nuevo el cuadro de diálogo y que se realice siempre

la acción seleccionada. Todavía no es posible usar algunos servicios y para otros es necesario instalar paquetes adicionales.

34.2.5 Ejemplos

En esta sección encontrará dos ejemplos de uso típicos de Bluetooth. El primero de ellos muestra cómo se puede establecer una conexión de red entre dos hosts usando Bluetooth. En la segunda, se describe una conexión entre un equipo y un teléfono móvil.

Conexión de red entre dos hosts

En el primer ejemplo, se establece una conexión de red entre los hosts *H1* y *H2.* Estos dos hosts cuentan con direcciones de dispositivo Bluetooth *baddr1* y *baddr2* (estas direcciones se averiguan en los dos hosts mediante el comando `hcitool dev`, tal y como se describe arriba). Los hosts deben identificarse con las direcciones IP `192.168.1.3` (*H1*) y `192.168.1.4` (*H2*).

La conexión Bluetooth se establece con la ayuda del daemon pand (daemon de red de área personal). Los siguientes comandos debe ejecutarlos el usuario `Root.` La descripción se centra en las acciones específicas de Bluetooth y no se proporciona una explicación detallada del comando de red `ip.`

Escriba `pand -s` para iniciar el daemon pand en el host *H1.* Posteriormente, se puede establecer una conexión con el host *H2* usando `pand -c baddr1.` Si especifica `ip link show` en uno de los hosts para mostrar las interfaces de red disponibles, el resultado debe contener una entrada como la siguiente:

```
bnep0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
 link/ether 00:12:34:56:89:90 brd ff:ff:ff:ff:ff:ff
```

En lugar de `00:12:34:56:89:90,` la salida debe contener la dirección del dispositivo local *baddr1* o *baddr2.* Ahora es necesario asignar a esta interfaz una dirección IP y, a continuación, activarla. En *H1,* esto se puede llevar a cabo con los dos comandos siguientes:

```
ip addr add 192.168.1.3/24 dev bnep0
ip link set bnep0 up
```

En *H2:*

```
ip addr add 192.168.1.4/24 dev bnep0
ip link set bnep0 up
```

Ahora se puede acceder a *H1* desde *H2* usando la dirección IP `192.168.1.3.` El comando `ssh 192.168.1.4` le permite acceder a *H2* desde *H1*, siempre que *H2* ejecute un sshd, que esté activado por defecto en SUSE Linux. El comando `ssh 192.168.1.4` también se puede ejecutar como un usuario normal.

Transmisión de datos de un teléfono móvil a un equipo

En este segundo ejemplo se va a mostrar cómo se transfiere una fotografía creada con un teléfono móvil con cámara digital incorporada a un equipo (sin incurrir en los costes adicionales de transmisión de un mensaje multimedia). Aunque cada teléfono móvil dispone de una estructura de menús diferente, el procedimiento será prácticamente el mismo en todos ellos. Si es necesario, consulte la documentación del teléfono. En este ejemplo se describe cómo se transfiere una fotografía desde un teléfono móvil Sony Ericsson a un portátil. Es necesario que el equipo disponga de servicio Obex-Push y que permita el acceso del teléfono móvil. En el primer paso, se activará el servicio en el equipo portátil. Necesita ejecutar en el portátil un daemon de servicio especial para poder obtener los datos del teléfono. Si el paquete `kbluetooth` está instalado, no tendrá que iniciar ningún daemon especial. Si `kbluetooth` no está instalado, utilice el daemon opd del paquete `bluez-utils`. Inicie el daemon con el siguiente comando:

```
opd --mode OBEX --channel 10 --daemonize --path /tmp --sdp
```

En este comando se utilizan dos parámetros importantes: `--sdp` registra el servicio sdpd y `--path /tmp` indica al programa dónde se deben guardar los datos recibidos (en este caso, en `/tmp`). Aquí también puede especificar otros directorios en los que tenga acceso de escritura.

Si utiliza kbluetooth, se le solicitará que indique un directorio cuando el portátil reciba la fotografía.

A continuación, el teléfono móvil debe ponerse en contacto con el equipo. Para ello, busque en el teléfono el menú *Connect* (Conexiones) y seleccione *Bluetooth.* Si es necesario, haga clic en *Turn On* (Activar) antes de seleccionar *My devices* (Mis dispositivos). Seleccione *New device* (Nuevo dispositivo) y deje que el teléfono busque el portátil. Si se detecta un dispositivo, su nombre aparecerá en la pantalla. Seleccione el dispositivo asociado al equipo portátil. Si se le solicita el número PIN, escriba el número especificado en `/etc/bluetooth/pin.` Ahora el teléfono y el portátil se reconocen y pueden intercambiar datos. Salga del menú actual y acceda al menú de imágenes. Seleccione la imagen que desee transferir y pulse *More* (Más). En el siguiente menú,

pulse *Send* (Enviar) para seleccionar un modo de transmisión. Seleccione *Via Bluetooth* (Mediante Bluetooth). El equipo portátil debe aparecer como dispositivo de destino. Seleccione el portátil para iniciar la transmisión. La imagen se guarda entonces en el directorio especificado con el comando `opd`. Este procedimiento también puede emplearse para transmitir un archivo de música.

34.2.6 Solución de problemas

En caso de que se produzcan problemas de conexión, se recomienda comprobar los siguientes puntos. No obstante, tenga siempre presente que el problema puede residir en cualquiera de los extremos de la conexión o, en el peor de los casos, en ambos. Si es posible, reproduzca el problema con un dispositivo Bluetooth distinto para asegurarse de que el dispositivo no esté dañado.

¿Aparece el dispositivo local en la salida de `hcitool dev`?
: Si el dispositivo local no aparece en la salida de este comando, es posible que hcid no se haya iniciado o que el dispositivo no se reconozca como dispositivo Bluetooth. Esto puede deberse a distintas causas: el dispositivo está estropeado o falta el controlador adecuado. En el caso de equipos portátiles con Bluetooth incorporado, suele haber un interruptor para dispositivos inalámbricos, como WLAN y Bluetooth. Consulte la documentación del portátil para ver si dispone de un interruptor de este tipo. Reinicie el sistema Bluetooth con `rcbluetooth restart` y examine el archivo `/var/log/messages` para ver si hay mensajes de error.

¿Necesita el adaptador Bluetooth un archivo de firmware?
: Si es así, instale `bluez-bluefw` y reinicie el sistema Bluetooth con `rcbluetooth restart`.

¿Aparecen en la salida de `hcitool inq` otros dispositivos?
: Ejecute este comando varias veces. La conexión puede tener interferencias porque la banda de frecuencia de Bluetooth también la utilizan otros dispositivos.

¿Coinciden los números PIN?
: Compruebe si el PIN del equipo (que aparece en `/etc/bluetooth/pin`) coincide con el del dispositivo de destino.

¿Puede "ver" el dispositivo remoto el equipo?
: Intente iniciar la conexión desde otro dispositivo remoto y compruebe si el dispositivo detecta la presencia del equipo.

¿Es posible establecer una conexión de red? Consulte “Conexión de red entre dos hosts” (p. 669).

La configuración descrita en “Conexión de red entre dos hosts” (p. 669) puede que no funcione por distintas causas. Por ejemplo, puede ser que uno de los dos equipos no admita el protocolo. Pruebe con el comando `ping 192.168.1.3` o con `ping 192.168.1.4`. Si esto funciona, compruebe si sshd está activo. Otra posible causa es que uno de los dos dispositivos disponga ya de unos ajustes de red que entren en conflicto con la dirección utilizada en el ejemplo `192.168.1.X`. Si es el caso, pruebe con direcciones distintas, como `10.123.1.2` o `10.123.1.3`.

¿Aparece el equipo portátil como dispositivo de destino? Consulte “Transmisión de datos de un teléfono móvil a un equipo” (p. 670). ¿Detecta el teléfono móvil el servicio Obex-Push en el equipo portátil?

En el menú *My devices* (Mis dispositivos), seleccione el dispositivo que corresponda y consulte la lista de servicios. Si en ella no aparece Obex-Push (incluso después de actualizar la lista), la causa del problema es opd en el portátil. ¿Está activo opd? ¿Tiene permiso de escritura en el directorio especificado?

¿Funciona a la inversa el ejemplo descrito en “Transmisión de datos de un teléfono móvil a un equipo” (p. 670)?

Si ha instalado el paquete `obexftp`, el comando `obexftp -b` *`dirección_dispositivo`* `-B 10 -p` *`imagen`* se puede usar en varios dispositivos. Algunos modelos de Siemens y Sony Ericsson se han probado y se ha confirmado que funcionan. Consulte la documentación de `/usr/share/doc/packages/obexftp`.

Si ha instalado el paquete `bluez-hcidump`, puede utilizar `hcidump -X` para comprobar lo que se envía de un dispositivo a otro. A veces la salida ayuda a determinar la causa del problema, pero tenga en cuenta que no todo se muestra como “texto legible”.

34.2.7 Información adicional

Para obtener información adicional de última hora, acceda a `/usr/share/doc/packages/bluez-utils/` (están disponibles las versiones en alemán e inglés).

Puede encontrar una amplia lista de documentación relacionada con el funcionamiento y la configuración de Bluetooth en `http://www.holtmann.org/linux/bluetooth/`. Otras fuentes de información:

- Procedimientos oficiales del stack del protocolo Bluetooth integrado en el núcleo: http://bluez.sourceforge.net/howto/index.html
- Conexión con dispositivo PDA PalmOS: http://www.cs.ucl.ac.uk/staff/s.zachariadis/btpalmlinux.html

34.3 Transmisión de datos mediante infrarrojos

IrDA (Asociación de datos por infrarrojos, del inglés Infrared Data Association) es un estándar industrial para las comunicaciones inalámbricas que utiliza infrarrojos. Muchos de los equipos portátiles actuales incorporan un emisor/receptor que permite la comunicación con otros dispositivos, tales como impresoras, módems, LAN u otros portátiles. La velocidad de transferencia oscila entre 2400 bps y 4 Mbps.

IrDA cuenta con dos modos de funcionamiento. El modo estándar SIR se comunica con el puerto infrarrojo a través de una interfaz en serie. Este modo funciona con casi todos los sistemas y cumple la mayoría de las exigencias. El modo más rápido FIR requiere un controlador especial para el chip IrDA, pero el modo FIR no admite todos los tipos de chips porque no existen controladores adecuados para todos ellos. En el BIOS del equipo hay que definir el modo IrDA que se desea usar. El BIOS también muestra qué interfaz en serie se utiliza en el modo SIR.

Hay más información disponible sobre IrDA en los procedimientos de Werner Heuser en http://tuxmobil.org/Infrared-HOWTO/Infrared-HOWTO.html. Si lo desea, también puede consultar el sitio Web del proyecto IrDA de Linux en http://irda.sourceforge.net/.

34.3.1 Software

Los módulos del núcleo necesarios se incluyen en el paquete del núcleo. El paquete `irda` contiene los programas de ayuda necesarios para que se pueda usar la interfaz infrarroja. Una vez instalado el paquete, podrá encontrar la documentación en `/usr/share/doc/packages/irda/README`.

34.3.2 Configuración

El servicio de sistema IrDA no se inicia automáticamente al arrancar el sistema, sino que debe activarse con el módulo IrDA de YaST. En este módulo sólo se puede modificar un ajuste: la interfaz en serie del dispositivo infrarrojo. La ventana de prueba está dividida en dos partes: una de ellas muestra la salida de `irdadump`, donde se registran todos los paquetes IrDA enviados y recibidos. En esta salida debe aparecer el nombre del equipo y los nombres de todos los dispositivos infrarrojos que haya en el radio de acción. Puede ver un ejemplo de estos mensajes en la Sección 34.3.4, “Solución de problemas” (p. 675). En la parte inferior de la pantalla se muestran todos los dispositivos con los que existe una conexión IrDA.

IrDA requiere bastante energía, puesto que envía un paquete Discovery cada pocos segundos con el fin de detectar otros dispositivos periféricos. Así pues, si trabaja con batería, se recomienda arrancar IrDA sólo cuando lo vaya a utilizar. Utilice el comando `rcirda start` para activarlo o `rcirda stop` para desactivarlo. Al activar la interfaz se cargarán automáticamente todos los módulos del núcleo necesarios.

La configuración manual se lleva a cabo en el archivo `/etc/sysconfig/irda`, que contiene sólo la variable `IRDA_PORT` que determina qué interfaz se va a usar en el modo SIR.

34.3.3 Uso

Los datos se pueden enviar al archivo de dispositivo `/dev/irlpt0` para su impresión. Este archivo se comporta igual que la interfaz normal con conexión `/dev/lp0`, con la salvedad de que los datos de impresión viajan mediante infrarrojos. A la hora de imprimir, asegúrese de que la impresora se encuentra en el área de visión de la interfaz infrarroja del equipo y de que la compatibilidad con infrarrojos está activada.

Una impresora que trabaja con la interfaz infrarroja puede configurarse mediante el módulo de impresión de YaST. Como no se detecta automáticamente, deberá realizar la configuración de forma manual haciendo clic en *Otro (no detectado)*. En el siguiente cuadro de diálogo, seleccione *Impresora IrDA*. Normalmente, `irlpt0` es la conexión adecuada. Hay más información disponible acerca del funcionamiento de las impresoras en Linux en el Capítulo 11, *Funcionamiento de la impresora* (p. 247).

El archivo de dispositivo `/dev/ircomm0` permite comunicarse con otros hosts, con teléfonos móviles o con otros dispositivos similares. Con la aplicación wvdial se puede

acceder a Internet mediante la interfaz infrarroja usando, por ejemplo, los teléfonos móviles Siemens S25 y Nokia 6210. También es posible sincronizar datos con el dispositivo Palm Pilot, siempre y cuando los ajustes del dispositivo de la aplicación correspondiente se hayan establecido en `/dev/ircomm0`.

Sólo es posible comunicarse con dispositivos que sean compatibles con la impresora o con los protocolos IrCOMM. A los dispositivos compatibles con el protocolo IROBEX como, por ejemplo, 3Com Palm Pilot, se puede acceder con aplicaciones especiales como irobexpalm e irobexreceive. Para obtener más información, consulte los procedimientos relacionados con los infrarrojos en *IR-HOWTO* (`http://tldp.org/HOWTO/Infrared-HOWTO/`). Los protocolos que admite el dispositivo aparecen entre corchetes después del nombre del dispositivo en la salida de `irdadump`. La compatibilidad con el protocolo IrLAN aún se encuentra "en desarrollo."

34.3.4 Solución de problemas

Si los dispositivos conectados al puerto infrarrojo no responden, use el comando `irdadump` (como usuario `Root`) para comprobar si el equipo detecta la presencia del otro dispositivo. Un resultado parecido al del Ejemplo 34.1, "Salida de irdadump" (p. 675) aparece normalmente cuando hay una impresora Canon BJC-80 en el rango de visión del equipo:

Ejemplo 34.1 *Salida de irdadump*

```
21:41:38.435239 xid:cmd 5b62bed5 > ffffffff S=6 s=0 (14)
21:41:38.525167 xid:cmd 5b62bed5 > ffffffff S=6 s=1 (14)
21:41:38.615159 xid:cmd 5b62bed5 > ffffffff S=6 s=2 (14)
21:41:38.705178 xid:cmd 5b62bed5 > ffffffff S=6 s=3 (14)
21:41:38.795198 xid:cmd 5b62bed5 > ffffffff S=6 s=4 (14)
21:41:38.885163 xid:cmd 5b62bed5 > ffffffff S=6 s=5 (14)
21:41:38.965133 xid:rsp 5b62bed5 < 6cac38dc S=6 s=5 BJC-80
                        hint=8804 [Printer IrCOMM ] (23)
21:41:38.975176 xid:cmd 5b62bed5 > ffffffff S=6 s=* earth
                        hint=0500 [ PnP Computer ] (21)
```

Si no aparece nada en pantalla o el otro dispositivo no responde, deberá comprobar la configuración de la interfaz. Asegúrese de que está usando la interfaz correcta. La interfaz infrarroja se encuentra a veces en `/dev/ttyS2` o en `/dev/ttyS3`, y puede que se use otra interrupción que no sea IRQ 3. Estos ajustes se pueden comprobar y modificar en la configuración del BIOS de casi todos los equipos portátiles.

Con una simple cámara de vídeo puede comprobar si el diodo LED se ilumina realmente; al contrario que los ojos humanos, la mayoría de las cámaras de vídeo pueden ver la luz infrarroja.

Índice

A

ACL, 155–167
  acceso, 158, 161
  algoritmo de comprobación, 166
  bits de permiso, 160
  compatibilidad, 167
  definiciones, 158
  efectos, 164
  estructura, 158
  gestión, 158
  máscaras, 162
  por defecto, 158, 164
actualización, 71–74
  mezcladores de sonido, 86
  passwd y group, 72
  problemas, 72
  YaST, 73
Administrador de volúmenes lógicos (ver LVM)
alternos (ver Squid)
  cachés, 559
  transparentes, 572
  ventajas, 559
Apache, 483–524
  configuración, 485
    archivos, 486
    asistente de HTTP de YaST, 493
    configuración del servidor HTTP con YaST, 498
    host virtual, 489
    manual, 485–493
    YaST, 493–500
  detención, 500
  guiones CGI, 510
  inicio, 500
  inicio rápido, 483
  instalación, 484
  más información, 523
  módulos, 502–510
    disponibles, 504
    generación de módulos, 509
    instalación, 503
    módulos de multiprocesamiento, 507–508
  resolución de problemas, 522
  seguridad, 520
  Squid, 575
  SSL, 513–519
    configuración de Apache con SSL, 518
    creación de un certificado SSL, 514
aplicaciones
  red
    remota, 311
  remotas
    FreeNX, 311
archivos
  búsqueda, 237
  cifrado, 129
  sincronización, 525–546
    CVS, 526, 535–538
    iFolder, 528
    mailsync, 527, 543–546
    rsync, 528
    Subversion, 527
    Unison, 526, 533–535
archivos de arranque
  menu.lst, 214
archivos de configuración, 381
  .bashrc, 234, 237
  .emacs, 239
  .mailsync, 544
  .profile, 234
  .xsession, 126
  acpi, 626
  configuración host, 384

crontab, 234
csh.cshrc, 244
dhclient.conf, 444
dhcp, 381
dhcpd.conf, 444
exports, 435–436
group, 72
grub.conf, 220
gshadow, 79
HOSTNAME, 388
hosts, 362, 383
idioma, 242, 244
ifcfg-*, 381
inittab, 197, 200, 240
inputrc, 241
irda, 674
kernel, 195
logrotate.conf, 236
modprobe.conf, 75
modules.conf, 75
named.conf, 406, 408–417, 565
nscd.conf, 387
nsswitch.conf, 385, 471
pam_unix2.conf, 470
passwd, 72
perfil, 244
permisos, 152
powersave, 625
powersave.conf, 84
profile, 233, 237
red, 381
redes, 384
resolv.conf, 239, 382, 406, 564
rutas, 381
samba, 551
servicios, 551, 573
slapd.conf, 461
smb.conf, 551, 558
smppd.conf, 390
smpppd-c.conf, 391
squid.conf, 564, 566, 570, 572, 575, 577
squidguard.conf, 577
sshd_config, 126
suseconfig, 209
sysconfig, 206–209
termcap, 241
wireless, 381
XF86Config, 88
xorg.conf, 88, 295
Device, 299
Monitor, 300
Screen, 298
archivos de núcleo central, 237
archivos de registro, 235
boot.msg, 625
mensajes, 120, 407
Squid, 565, 568, 574
Unison, 535
XFree86, 309
arranque, 193
configuración
YaST, 222–227
GRUB, 211–232
gráfica, 229
initramfs, 195
initrd, 195
sectores de arranque, 211–212
asistencia de instalación
tarjetas gráficas 3D, 309
autenticación
Kerberos, 87
PAM, 325–333
ayuda
páginas Man, 239
X, 301

B

Bash

.bashrc, 234
.profile, 234
profile, 233
BIND, 406–417
Bluetooth, 590, 661
hciconfig, 668
hcitool, 667
opd, 670
pand, 669
red, 665
sdptool, 668

C

cámaras digitales, 591
centralita, 370
chown, 78
cifrado, 127–130
archivos, 129–130
creación de particiones, 128
de archivos con vi, 130
medios extraíbles, 130
particiones, 128–129
UTF-8, 78
YaST, 128
CJK, 241
codificación
ISO-8859-1, 243
comandos
chown, 78
fonts-config, 302
free, 238
getfacl, 162
grub, 212
head, 78
ldapadd, 467
ldapdelete, 470
ldapmodify, 469
ldapsearch, 469
lp, 257
nice, 78
rpm, 94
rpmbuild, 94
scp, 122
setfacl, 162
sftp, 123
slptool, 395
smbpasswd, 557
sort, 78
ssh, 122
ssh-agent, 126
ssh-keygen, 125
tail, 78
conexiones inalámbricas
Bluetooth, 661
configuración, 206
DNS, 365, 397
DSL, 372
encaminamiento, 381
GRUB, 212, 220
impresión, 251–254
IPv6, 360
IrDA, 674
módem de cable, 371
módems, 366
PAM, 89
redes, 363
manual, 377–389
RSDI, 368
Samba, 549–555
clientes, 555
Squid, 566
SSH, 121
T-DSL, 374
configuración regional
UTF-8, 78
consolas
asignación, 240
cambio, 240
gráficas, 229

control remoto
FreeNX, 311–323
correo electrónico
sincronización, 527, 589
mailsync, 543–546
cortafuegos, 109
filtros de paquetes, 109, 114
Squid, 573
SuSEfirewall2, 109, 115
cpuspeed, 634
cron, 234
CVS, 526, 535–538

D

deltarpm, 98
desinstalación
GRUB, 228
Linux, 228
DHCP, 439–448
asignación de direcciones estáticas, 446
configuración con YaST, 440
dhcpd, 444–446
paquetes, 444
servidor, 444–446
direcciones IP, 348
asignación dinámica, 439
clases, 349
enmascaramiento, 112
IPv6, 351
configuración, 360
privadas, 351
discos
arranque, 228
dispositivos PDA, 592
DNS, 361
BIND, 406–417
configuración, 365, 397
dominio de nivel superior, 361
dominios, 382
inicio, 407
intercambiador de correo, 362
multidifusión, 77
NIC, 362
opciones, 409
registro, 410
remisión, 407
resolución de problemas, 407
resolución inversa, 416
seguridad y, 150
servidores de nombre, 382
Squid, 565
terminología, 397
zonas
archivos, 412
dominios
.local, 77
DOS
uso compartido de archivos, 547

E

editores
Emacs, 239–240
Emacs, 239–240
.emacs, 239
default.el, 240
encaminamiento, 348, 381–382
estático, 382
máscaras de red, 349
rutas, 381
enmascaramiento, 112
configuración con SuSEfirewall2, 115
enrutamiento
enmascaramiento, 112
Evolution, 592

F

filtros de paquetes (ver cortafuegos)
Firefox

comando de apertura de URL, 93
Firewire (IEEE1394)
discos duros, 591
FreeNX, 311–323
fuente
compilación, 102
fuentes, 302
centrales X11, 302
con clave CID, 306
TrueType, 301
Xft, 303

G

gestión de energía, 583, 621–643
ACPI, 621, 625–633, 638
APM, 621, 623–625, 638
cpufrequency, 634
cpuspeed, 634
hibernación, 622
monitorización de la batería, 623
nivel de carga, 639
powersave, 634
stand-by, 622
suspensión, 622
YaST, 644
GRUB, 211–232
arranque, 212
comandos, 212–222
contraseña de arranque, 221
desinstalación, 228
device.map, 213, 219
editor de menú, 218
error de geometría de GRUB, 230
grub.conf, 213, 220
JFS y GRUB, 230
limitaciones, 212
menú de arranque, 214
menu.lst, 213–214
nombres de dispositivos, 216
nombres de particiones, 216
Registro de arranque principal (MBR), 211
sectores de arranque, 212
solución de problemas, 230
gráficos
3D, 307–310
3Ddiag, 309
asistencia para la instalación, 309
compatibilidad, 307
controladores, 307
diagnóstico, 308
pruebas, 308
SaX, 308
solución de problemas, 309
GLIDE, 307–310
OpenGL, 307–310
controladores, 307
pruebas, 308
tarjetas
3D, 307–310
controladores, 300
guiones
init.d, 197, 200–204, 388
boot, 202
boot.local, 202
boot.setup, 202
halt, 203
nfsserver, 388, 435
portmap, 388, 435
rc, 200, 203
red, 388
sendmail, 389
squid, 564
xinetd, 388
ypbind, 389
ypserv, 389
irda, 674
mkinitrd, 195
modify_resolvconf, 239, 383

SuSEconfig, 206–209
inhabilitación, 209

H

hardware
RSDI, 368
hciconfig, 668
hcitool, 667
head, 78
hojas de estilo TEI XSL
nueva ubicación, 92

I

I18N, 242
iFolder, 528
impresión, 247, 251–254
aplicaciones, desde, 257
archivo PPD, 252
colas, 252
conexión, 252
configuración con YaST, 251
controlador Ghostscript, 252
controladores, 252
CUPS, 258
impresoras GDI, 264
IrDA, 674
kprinter, 258
línea de comandos, 257
página de prueba, 252
puerto, 252
red, 266
Samba, 548
solución de problemas
red, 266
xpp, 258
init, 197
adición de guiones, 203
guiones, 200–204
inittab, 197
instalación
GRUB, 212
manual, 87
paquetes, 95
internacionalización, 242
Internet
acceso telefónico, 389–391
cinternet, 390
DSL, 372
KInternet, 390
qinternet, 390
RSDI, 368
smpppd, 389–391
TDSL, 374
IrDA, 590, 673–676
configuración, 674
detención, 674
inicio, 674
resolución de problemas, 675

K

kernels
cachés, 238
Kontact, 592
KPilot, 592
KPowersave, 587
KSysguard, 588

L

L10N, 242
LDAP, 455–481
ACL, 462
adición de datos, 466
administración de grupos, 479
administración de usuarios, 479
búsqueda de datos, 469
cliente LDAP de YaST, 470
configuración del servidor, 461
control de acceso, 464

ldapadd, 466
ldapdelete, 470
ldapmodify, 468
ldapsearch, 469
modificación de datos, 468
supresión de datos, 470
YaST
módulos, 472
plantillas, 472
árbol de directorios, 458
LFS, 290
Linux
desinstalación, 228
redes y, 345
uso compartido de archivos con otro SO, 547
Linux de 64 bits, 189
asistencia sobre tiempo de ejecución, 189
desarrollo de software, 190
especificaciones de núcleo, 192
linuxrc
instalación manual, 87
linuxthreads, 76
localización, 242
locate, 237
logrotate, 235
LSB
instalación de paquetes, 94
LVM
YaST, 57

M

MBR, 211–212
medios extraíbles
subfs, 81
memoria
RAM, 238
módems
cable, 371
YaST, 366
módulos de autenticación conectables (ver PAM)
monitorización del sistema, 587
KPowersave, 587
KSysguard, 588
mountd, 436
movilidad, 583–593
cámaras digitales, 591
discos duros externos, 591
dispositivos PDA, 592
Firewire (IEEE1394), 591
portátiles, 583
seguridad de los datos, 590
teléfonos móviles, 592
USB, 591

N

NAT (ver enmascaramiento)
NetBIOS, 547
NetworkManager, 586
NFS, 431
clientes, 431
exportación, 434
importación, 432
montaje, 432
permisos, 435
servidores, 433
nfsd, 436
NGPT, 76
nice, 78
NIS, 421–429
clientes, 428
esclavo, 421–428
principal, 421–428
niveles de ejecución, 197–200
cambio, 199–200
edición en YaST, 204

Novell iFolder, 528
NPTL, 76
NSS, 385
  bases de datos, 386
núcleos
  límites, 291
  módulos
    modprobe.conf, 75
  versión 2.6, 75

O

opd, 670
OpenLDAP (ver LDAP)
OpenSSH (ver SSH)
OS/2
  uso compartido de archivos, 547

P

páginas Man, 239
PAM, 325–333
  configuración, 89
pand, 669
pantalla
  resolución, 299
paquetes
  compilación, 102
  compilación con build, 104
  comprobación, 94
  desintalación, 95
  gestor de paquetes, 94
  instalación, 95
  LSB, 94
  RPM, 94
paquetes de hilos
  NPTL, 76
particiones
  cifrado, 128
  tabla de partición, 211
PCMCIA, 583, 595
  IrDA, 673–676
permisos
  ACL, 155–167
  permisos de archivo, 236
portátiles, 583–591, 595 (ver equipo portátil)
  gestión de energía, 583, 621–634
  hardware, 583
  IrDA, 673–676
  NetworkManager, 586
  PCMCIA, 583
  SCPM, 584, 605
  SLP, 587
ports
  53, 409
PostgreSQL
  actualización, 72
powersave, 634
  configuración, 635
Protocolo de ubicación de servicios (ver SLP)
protocolo ligero de acceso al directorio (ver LDAP)
protocolos
  CIFS, 547
  IPv6, 351
  LDAP, 455
  SLP, 393
  SMB, 547
puertos
  exploración, 574

R

RAID
  YaST, 64
RAID de software (ver RAID)
redes, 345
  archivos de configuración, 381–388
  Bluetooth, 590, 665

configuración, 362–374, 377–389
IPv6, 360
DHCP, 439
dirección de difusión, 350
dirección de red básica, 350
DNS, 361
encaminamiento, 348–349
host local, 351
inalámbricas, 589
IrDA, 590
máscaras de red, 349
SLP, 393
TCP/IP, 345
WLAN, 589
YaST, 363
Registro de arranque principal (ver MBR)
RFC, 345
RPM, 94–105
actualización, 95
base de datos
reconstrucción, 96, 102
comprobación, 94
consultas, 99
deltarpm, 98
dependencias, 95
desintalación, 96
herramientas, 105
revisiones, 96
rpmnew, 95
rpmorig, 95
rpmsave, 95
seguridad, 152
SRPMS, 103
verificar, 101
rpmbuild, 94
rsync, 528, 541

S

Samba, 547–558
CIFS, 547
clientes, 548, 555–556
configuración, 549–555
detención, 549
impresión, 556
impresoras, 548
inicio, 549
inicio de sesión, 556
instalación, 549
nombres, 547
permisos, 554
recursos compartidos, 548, 552
relación con TCP/IP, 547
seguridad, 554–555
servidor, 548
servidores, 549–555
SMB, 547
swat, 551
SCPM, 605
ajustes avanzados, 616
cambio de perfiles, 616
gestión de perfiles, 615
grupos de recursos, 614
inicio, 614
portátiles, 584
sdptool, 668
seguridad, 140–154
arranque, 141–144
ataques, 149–150
consejos y trucos, 151
contraseñas, 142–143
cortafuegos, 109
detección de intrusiones, 88
DNS, 150
errores y, 145, 148
firmas RPM, 152
gusanos, 150
ingeniería, 141
local, 142–146
notificación de problemas, 153

permisos, 144–145
red, 146–150
Samba, 554
sistema de archivos cifrado, 590
Squid, 560
SSH, 121–127
tcpd, 153
telnet, 121
terminales en serie, 141–142
virus, 146
X y, 147
seguridad de los datos, 590
Servicio de información de red (ver NIS)
servidores de nombres (ver DNS)
SGML
directorios, 81
sincronización de datos, 589
correo electrónico, 589
Evolution, 592
Kontact, 592
KPilot, 592
sistema
actualización, 71–74
limitación del uso de recursos, 237
localización, 242
sistema de archivos en red (ver NFS)
sistema de nombres de dominio (ver DNS)
sistema X Window (ver X)
sistemas de archivos, 281–292
ACL, 155–167
cifrado, 127
compatibles, 289–290
cryptofs, 127
Ext2, 284
Ext3, 285–286
LFS, 290
limitaciones, 290
Reiser4, 286–287
ReiserFS, 283
selección, 282
términos, 281
XFS, 287–289
SLP, 393, 587
Konqueror, 395
navegador, 395
servicios de registro, 393
slptool, 395
SMB (ver Samba)
smpd, 547
software
compilación, 102
sonido
mezcladores, 86
sort, 78
spm, 102
Squid, 559
ACL, 569
alternos transparentes, 572, 574
Apache, 575
archivos de registro, 565, 568, 574
cachemgr.cgi, 575–576
cachés, 559–560
daños, 565
tamaño, 562
Calamaris, 578–579
configuración, 566
controles de acceso, 575
cortafuegos, 573
CPU, 563
desinstalación, 565
detención, 564
directorios, 564
DNS, 565
estado de objetos, 561
estadísticas, 575–576
funciones, 559
informes, 578–579
inicio, 564
permisos, 564, 569
RAM, 563

requisitos del sistema, 562
seguridad, 560
solución de problemas, 565
squidGuard, 577
SSH, 121–127
daemon, 123
mecanismos de autenticación, 125
pares de claves, 123, 125
scp, 122
sftp, 123
ssh, 122
ssh-agent, 126
ssh-keygen, 125
sshd, 123
X, 126
subfs
medios extraíbles, 81
Subversion, 527, 538
SVN (Subversion), 527

T

tail, 78
tarjetas
gráficas, 300
red, 362–363
TCP/IP, 345
ICMP, 346
IGMP, 346
modelo de capa, 346
paquetes, 347–348
TCP, 346
UDP, 346
teclado
caracteres asiáticos, 241
diseño, 241
distribución, 241
compose, 241
tecla compuesta, 241
X Keyboard Extension, 241
XKB, 241
teléfonos móviles, 592
Tripwire
sustitución por AIDE, 88

U

ulimit, 237
opciones, 237
unidades flash, 591
USB
discos duros, 591
unidades flash, 591
usuarios
/etc/passwd, 328, 471
UTF-8
cifrado, 78

V

variables
entorno, 242

W

whois, 362
Windows
uso compartido de archivos, 547
WLAN, 589

X

X
ayuda, 301
conjuntos de caracteres, 301
controladores, 300
fuentes, 301
fuentes centrales X11, 302
fuentes con clave CID, 306
fuentes TrueType, 301
optimización, 295–301
pantalla virtual, 299
SaX2, 296

seguridad, 147
sistemas de fuentes, 302
SSH, 126
xf86config, 296
xft, 301
Xft, 303
X Keyboard Extension (ver teclado, XKB)
X.Org, 295
Xen, 335
descripción general, 335
Xft, 303
XKB (ver teclado, XKB)
XML
directorios, 81
xorg.conf
Depth, 298
Device, 298
Display, 298
Files, 296
InputDevice, 296
Modeline, 299
modelines, 297
Modes, 297, 299
Monitor, 297–298
profundidad de color, 299
ServerFlags, 296

Y

YaST
3D, 307
actualización, 73
cable de módem, 371
cargador de arranque
contraseña, 226
orden de los discos, 227
tipo, 223
ubicación, 224
cliente LDAP, 470
cliente NIS, 428
configuración de arranque
seguridad, 226
sistema por defecto, 225
tiempo límite, 226
configuración del arranque, 222
DHCP, 440
DSL, 372
editor sysconfig, 207
gestión de energía, 644
GRUB, 223
impresión, 251–254
LILO, 223
LVM, 57
módems, 366
navegador SLP, 395
niveles de ejecución, 204
RAID, 64
RSDI, 368
Samba
clientes, 555
T-DSL, 374
tarjeta de red, 363
YP (ver NIS)