



SuSE Linux

MANUAL DE ADMINISTRACIÓN

2ª edición 2004

Copyright ©

Esta obra es propiedad intelectual de SuSE Linux AG.

Se permite su reproducción total o parcial siempre que cada una de las copias contenga esta nota de copyright.

Toda la información contenida en este libro ha sido compilada minuciosamente. Sin embargo, no es posible excluir cualquier tipo de error. Los autores, traductores y SuSE Linux AG no se hacen responsables de posibles errores ni aceptarán responsabilidad jurídica alguna derivada de estos errores o sus consecuencias.

Los productos de software o hardware mencionados en este libro son en muchos casos marcas registradas. SuSE Linux AG se atiene esencialmente a la grafía de los fabricantes.

La reproducción de nombres comerciales, marcas registradas, etc. en este documento no justifica, aún sin una indicación explícita, la suposición de que tales nombres se puedan considerar como libres según la legislación de nombres comerciales y protección de marcas.

Dirija sus comentarios y sugerencias a documentation@suse.de

Autores: Frank Bodammer, Stefan Dirsch, Olaf Donjak, Torsten Duwe, Roman Drahtmüller, Thorsten Dubiel, Karl Eichwalder, Thomas Fehr, Stefan Fent, Werner Fink, Kurt Garloff, Carsten Groß, Andreas Grünbacher, Franz Hassels, Andreas Jaeger, Klaus Kämpf, Hubert Mantel, Anas Nashif, Johannes Meixner, Lars Müller, Matthias Nagorni, Peter Pöml, Siegfried Olschner, Heiko Rommel, Marcus Schaefer, Nikolaus Schüler, Klaus Singvogel, Hendrik Vogelsang, Klaus G. Wagner, Christian Zoz

Traducción: Inés Pozo Muñoz

Redacción: Jörg Arndt, Antje Faber, Berthold Gunreben, Roland Haidl, Jana Jaeger, Edith Parzefall, Peter Reinhart, Thomas Rölz, Marc Rührschneck, Thomas Schraitle, Rebecca Walter

Diseño: Manuela Piotrowski, Thomas Schraitle

Composición: L^AT_EX

Este libro fue impreso sobre papel blanqueado 100 % libre de cloro.

Índice general

Introducción	1
Novedades del Manual de Administración	2
Convenciones tipográficas	3
Agradecimientos	3

I Instalación 5

1. La instalación 7

Instalación en modo texto con YaST	8
La pantalla de bienvenida	8
La base: linuxrc	10
Iniciar SuSE Linux	16
Instalaciones especiales	18
Consejos y trucos	21
Crear un disquete de arranque bajo DOS	21
Crear un disquete de arranque bajo un sistema tipo Unix	22
Arrancar con un disquete (SYSLINUX)	23
Arrancar con el CD 2	24
¿Soporta Linux mi lector CD-ROM?	24
Un lector CD-ROM ATAPI se traba leyendo	25
Particionar para usuarios avanzados	26
El tamaño de la partición de intercambio (swap)	27

Formas de uso del ordenador	27
Posibilidades de optimización	29
Configuración de LVM con YaST	31
Gestor de volúmenes lógicos (LVM)	32
Configurar el LVM con YaST	33
LVM – Particionador	34
LVM – Configuración de los volúmenes físicos	36
Volúmenes lógicos	37
Soft-RAID	39
Niveles de RAID habituales	39
Configurar un Soft-RAID con YaST	41
2. Actualización del sistema – Gestión de paquetes	43
Actualización de SuSE Linux	44
Preparativos	44
Actualización con YaST	46
Actualización manual	46
Actualización de paquetes individuales	49
Cambio del software de una versión a otra	49
De 7.3 a 8.0	50
De la 8.0 a la 8.1	51
De 8.1 a 8.2	52
De 8.2 a 9.0	53
RPM – El gestor de paquetes	54
Comprobar la autenticidad de un paquete	55
Instalar, actualizar y desinstalar paquetes.	55
RPM y parches	57
Realizar consultas	59
Instalar y compilar los paquetes fuente	62
Creación de paquetes RPM con build	64
Herramientas para los archivos RPM y la base de datos RPM	64

II Configuración	65
3. YaST en modo texto (ncurses)	67
Funcionamiento	68
Trabajar con los módulos	69
Arranque de módulos individuales	70
La actualización online de YaST	71
4. El proceso de arranque y el gestor de arranque	73
El proceso de arranque en el PC	74
Sectores de arranque	74
Concepto de arranque	75
Archivos map, GRUB y LILO	76
El arranque con GRUB	77
El menú de arranque de GRUB	78
El archivo device.map	83
El archivo /etc/grub.conf	84
Definir la contraseña de arranque	85
Posibles problemas e información adicional	86
Arrancar con LILO	87
Fundamentos	87
Configuración de LILO	88
El contenido del archivo lilo.conf	89
Instalar y desinstalar LILO	92
Recuperar el MBR (Windows 2000)	94
Arrancar Linux después de recuperar el MBR	95
Crear un CD de arranque	95
CD de arranque con ISOLINUX	96

5. El sistema X Window	99
Historia de XFree86	100
La versión 4.x de XFree86	101
Configuración con xf86config	102
Optimizar la instalación del sistema X Window	111
Incorporar fuentes (TrueType) adicionales	117
Configuración de OpenGL/3D	120
Hardware Soportado	120
Herramienta de diagnóstico 3Ddiag	122
Aplicaciones de prueba OpenGL	122
Soporte de instalación	123
Documentación on line adicional	123
6. Funcionamiento de la impresora	125
Fundamentos del proceso de impresión	126
Ejemplos de lenguajes de impresión estándar	126
Desarrollo de un trabajo de impresión	126
Distintos sistemas de impresión	129
Requisitos para imprimir	129
Requisitos generales	129
Determinar el controlador de impresión correcto	130
La problemática de las impresoras GDI	132
Configuración de impresoras con YqST	134
Colas de impresión y configuración	134
Fundamentos de la configuración de impresoras con YqST	134
Configuración automática	136
Configuración manual	137
Configuración para aplicaciones	140
Configuración manual de puertos locales	140
Puertos paralelos	140
Puerto USB	143
Puerto IrDA	144

Puertos serie	145
Configuración manual de LPRng/lpfilter	145
El spooler de impresión LPRng	146
Imprimir desde aplicaciones	147
Herramientas de línea de comandos para LPRng	147
Para colas de impresión locales	147
Para colas de impresión remotas	150
Resolución de problemas con los comandos anteriores en LPRng	151
El filtro de impresión del sistema LPRng/lpfilter	152
Configuración de lpfilter	154
Complementos para lpfilter	154
Búsqueda de errores en lpfilter	160
El sistema de impresión CUPS	161
Convenciones lingüísticas	161
IPP y servidor	161
Configuración del servidor CUPS	162
Impresoras de red	164
Procesamiento interno de los trabajos	165
Consejos y trucos	166
Imprimir desde aplicaciones	168
Herramientas de línea de comandos para el sistema de impresión CUPS	169
Para colas de impresión locales	169
Colas de impresión en red	172
Resolución de problemas en CUPS con los comandos anteriores	172
Acerca de Ghostscript	173
Ejemplos de trabajo con Ghostscript	174
Acerca de a2ps	177
Impresión directa de un archivo de texto con a2ps	177
Reformatear PostScript con psutils	178
psnup	178
pstops	178
psselect	181

Control en la pantalla con Ghostscript	181
Codificación de texto ASCII	181
Ilustración	182
Impresión en redes TCP/IP	183
Aclaración de términos	183
Configuración rápida de un cliente	184
Protocolos para imprimir en una red TCP/IP	186
Filtros en la impresión en red	192
Resolución de problemas	196
Servidor de impresión LPD e IPP	201
7. Hotplug	203
Hotplug en Linux	204
Arrancar Hotplug y Coldplug	204
USB	205
PCI y PCMCIA	206
Red	207
Otros dispositivos y el desarrollo posterior	208
8. Ordenadores portátiles – PCMCIA, APM, IrDA	209
PCMCIA	210
El hardware	210
El software	210
La configuración	212
Configuración variable - SCPM	214
Si aún no funciona	215
Instalación vía PCMCIA	219
Utilidades adicionales	220
Actualizar el paquete Kernel o PCMCIA	220
Información adicional	221
SCPM – System Configuration Profile Management	222
Fundamentos y conceptos básicos	222
El gestor de perfiles de YaST y documentación adicional	223

Configurar SCPM	224
Crear y administrar perfiles	224
Cambiar de un perfil a otro	225
Configuración avanzada del perfil	226
Selección de perfiles al arrancar	227
Problemas y soluciones	229
APM y ACPI – Powermanagement	230
Funciones para el ahorro de energía	230
APM	232
El daemon APM (apmd)	233
Comandos adicionales	234
ACPI	234
Parar el disco duro	243
IrDA – Infrared Data Association	244
Software	245
Uso	245
Solución de problemas	246

III El sistema 249

9. SuSE Linux en sistemas AMD64	251
SuSE Linux de 64 bits para AMD64	251
Hardware	251
Software	252
Instalación de software de 32 bits	252
Desarrollo de software en sistemas de 64 bits	252
Información adicional	253

10. El kernel de Linux	255
Actualización del kernel	256
Las fuentes del kernel	257
Configuración del kernel	257
Módulos del kernel	259
Ajustes en la configuración del kernel	262
Compilación del kernel	262
Instalación del kernel	263
Limpieza del disco después de la compilación	264
 11. Características del sistema	 265
Estándares de Linux	266
Filesystem Hierarchy Standard (FHS)	266
Linux Standard Base (LSB)	266
teTeX – TeX en SuSE Linux	266
Entornos de ejemplo para FTP y HTTP	266
Observaciones sobre paquetes especiales	267
El paquete bash y /etc/profile	267
El paquete cron	268
Archivos de registro – el paquete logrotate	268
Páginas man	270
El comando ulimit	270
El comando free	271
El fichero /etc/resolv.conf	272
Configuración de GNU Emacs	272
Arrancar con initial ramdisk	273
El concepto “initial ramdisk”	274
Procedimiento del arranque con initrd	274
Cargadores de arranque	275
Uso de initrd en SuSE	276
Posibles problemas – Kernel compilado a medida	277
El futuro	278

linuxrc	278
El sistema de rescate de SuSE	283
Iniciar el sistema de rescate	285
Trabajar con el sistema de rescate	287
Consolas virtuales	289
Distribución del teclado	289
Configuración nacional – I18N/L10N	291
12. El concepto de arranque de SuSE Linux	295
El programa init	296
Los niveles de ejecución – “runlevels”	296
Cambio de nivel de ejecución	298
Los scripts de inicio	299
Añadir scripts init	301
El editor de niveles de ejecución de YaST	303
SuSEconfig y /etc/sysconfig	304
El editor Sysconfig de YaST	306
 IV La red	 309
13. Fundamentos de conexión a redes	311
TCP/IP - El protocolo de red utilizado por Linux	312
Modelo de capas	313
Direcciones IP y routing	316
Domain Name System	319
IPv6 – La próxima generación de Internet	320
El por qué del nuevo protocolo de Internet	320
Estructura de una dirección IPv6	322
Máscaras de red en IPv6	324
Literatura y enlaces sobre IPv6	324
El acceso a la red	326
Preparativos	326

Configuración de red con YaST2	326
Hotplug/PCMCIA	328
Configurar IPv6	328
Configuración manual de la red	329
Archivos de configuración	330
Scripts de arranque (ingl. <i>Startup-Scripts</i>)	336
Routing en SuSE Linux	337
DNS – Domain Name System	339
Iniciar el servidor de nombres BIND	339
El archivo de configuración /etc/named.conf	340
Transacciones seguras	348
Actualización dinámica de los datos de zonas	349
DNSSEC	349
Información adicional	350
El servicio de directorio LDAP	351
LDAP contra NIS	353
Estructura de un árbol de directorios LDAP	354
Configuración de servidor con slapd.conf	356
Administración de datos en el directorio LDAP	361
Configuración de LDAP con YaST	366
Información adicional	374
NIS – Network Information Service	377
Servidores NIS: maestro y esclavo	377
El módulo del cliente NIS en YaST	379
NFS – Sistema de archivos distribuidos	382
Importar sistemas de archivos con YaST	382
Importar sistemas de archivos manualmente	382
Exportar sistemas de archivos con YaST	383
Exportar manualmente sistemas de archivos	383
DHCP	387
El protocolo DHCP	387
Los paquetes de software DHCP	387

El servidor DHCP: dhcpd	388
Ordenadores con direcciones IP fijas	390
Información adicional	391
Sincronización horaria con xntp	392
Introducción	392
Configuración en red	392
Instalar un reloj de referencia local	393
14. El servidor web Apache	395
¿Qué es un servidor web?	395
Servidor web	395
HTTP	395
URLs	395
Reproducción automática de una página predeterminada	396
¿Qué es Apache?	397
El servidor web de uso más extendido	397
Ampliable	397
Personalizable	397
Estable	397
Prestaciones	398
Fundamentos	398
Diferencias entre Apache 1.3 y Apache 2	399
Resumen	399
¿Qué es una hebra o thread?	400
Hebras y procesos	400
Conclusión	401
Instalación	401
Selección de paquetes en YaST	401
Activar Apache	401
Módulos para contenidos activos	402
Paquetes suplementarios	402
Instalación de módulos con Apxs	402

Configuración	403
¿Debo configurar en absoluto?	403
Configuración con SuSEconfig	403
Configuración manual	404
Funcionamiento de Apache	409
¿Dónde se guardan las páginas y scripts?	409
Estado de Apache	409
Contenidos activos	410
Información general	410
Comparación entre el intérprete de scripts como módulo y CGI	411
SSI	411
CGI	412
¿Qué es CGI?	412
Ventajas de CGI	412
GET y POST	412
Lenguajes para CGI	412
¿Dónde se guardan los scripts?	413
Crear contenidos activos con módulos	413
Módulos para lenguajes de scripts	413
mod_perl	414
mod_php4	416
mod_python	417
mod_ruby	417
Máquinas virtuales	417
Introducción a las máquinas virtuales	417
Máquinas virtuales en función del nombre	418
Máquinas virtuales en función de la dirección IP	419
Múltiples instancias de Apache	421
Seguridad	421
El método más seguro: ningún servidor	421
Permisos de acceso	421
Siempre al día	422

Identificación y resolución de problemas	422
Documentación adicional	423
Apache	423
CGI	424
Seguridad	424
Fuentes adicionales	425
15. Sincronización de ficheros	427
Software para sincronizar datos	428
Inter-Mezzo	428
unison	429
CVS	429
mailsync	429
Criterios para la elección de programa	430
Cliente-servidor o igualdad de derechos	430
Portabilidad	430
Interactivo o automático	430
Velocidad	431
Conflictos: cuando aparecen y cómo resolverlos	431
Seleccionar y añadir ficheros	431
Historia	432
Cantidad de datos y requisitos de espacio	432
GUI	432
Requisitos que debe cumplir el usuario	432
Seguridad frente a agresiones externas	433
Seguridad frente a pérdida de datos	433
Introducción a InterMezzo	434
Arquitectura	434
Configuración de un servidor InterMezzo	435
Configuración de clientes InterMezzo	436
Resolución de problemas	436
Introducción a unison	437

Campos de aplicación	437
Requisitos	437
Manejo	437
Información adicional	439
Introducción a CVS	439
Campos de aplicación	439
Configuración del servidor CVS	439
Manejo de CVS	440
Información adicional	442
Introducción a mailsync	442
Campos de aplicación	442
Configuración y manejo	442
Posibles problemas	445
Información adicional	445
16. Redes heterogéneas	447
Samba	448
Instalación y configuración del servidor	449
Samba como servidor de dominio	453
Instalación de los clientes	455
Optimización	455
Netatalk	457
Configuración del servidor de archivos	458
Configuración del servidor de impresión	462
Arrancar el servidor	462
Emulación de Novell Netware con MARSNWE	464
Iniciar el emulador de netware MARSNWE	464
El fichero de configuración /etc/nwserv.conf	464
Administración de servidores Netware	467
Router de IPX mediante ipxrip	468

17. Internet	469
smpppd como asistente para la conexión telefónica	470
Componentes del programa para la conexión a Internet vía tele- fónica	470
La configuración de smpppd	470
Preparación de kinternet y cinternet para el uso remoto	471
Configuración de una conexión ADSL	472
Configuración estándar	472
Conexión ADSL vía "Dial-on-Demand"	473
Servidor proxy: Squid	474
¿Qué es un caché proxy?	474
Información general sobre cachés proxy	475
Requerimientos del sistema	476
Arrancar Squid	478
El archivo de configuración /etc/squid/squid.conf	480
Configuración de un proxy transparente	485
Squid y otros programas	488
Información adicional sobre Squid	493
18. Seguridad en la red	495
Cortafuegos y masquerading	496
Fundamentos del masquerading	496
Fundamentos del cortafuegos	498
SuSEfirewall2	499
SSH – secure shell, la alternativa segura	502
El paquete OpenSSH	503
El programa ssh	503
scp – copiar de forma segura	504
sftp - transmisión segura de datos	504
El daemon SSH (sshd) – el lado del servidor	504
Mecanismos de autenticación de SSH	506
"X", autenticación remota y mecanismos de reenvío	507

Autenticación en la red — Kerberos	508
Terminología de Kerberos	509
¿Cómo funciona?	510
Efectos de Kerberos a nivel de usuario	513
Información adicional sobre Kerberos	514
Instalación y administración de Kerberos	515
Elección de Realms en Kerberos	515
Configuración del hardware KDC	516
Sincronización del reloj	517
Configuración del registro	518
Instalación del KDC	518
Configuración de los clientes Kerberos	521
Configuración de la administración remota	524
Creación de principales de host en Kerberos	526
Activación del soporte PAM para Kerberos	527
Configuración de SSH para la autenticación con Kerberos	528
Utilización de LDAP y Kerberos	529
La seguridad, una cuestión de confianza	532
Conceptos básicos	532
Seguridad local y seguridad en la red	533
Trucos y consejos: indicaciones generales	542
Informe a SuSE sobre nuevos problemas de seguridad	544
 V Anexo	 545
A. Sistemas de archivos en Linux	547
Glosario	547
Los sistemas de archivos más importantes en Linux	548
Ext2	548
Ext3	549
ReiserFS	551
JFS	552
XFS	553
Otros sistemas de archivos soportados	554
Soporte de archivos grandes en Linux	555
Información adicional	557

B. Listas de control de acceso (ACLs) en Linux	559
¿Por qué ACLs?	560
Definiciones	561
Funcionamiento de las ACLs	561
Estructura de las entradas ACL	562
Entradas ACL y bits de permiso	563
Un directorio con access ACL	564
Directorios con ACLs predeterminadas	567
Evaluación de una ACL	570
El futuro de las ACLs	571
C. Página man de e2fsck	573
D. Página man de reiserfsck	577
E. La licencia pública general GNU (GPL)	581
Bibliografía	591

Introducción

El *Manual de Administración* le permite profundizar en la técnica de SuSE Linux y conocer los detalles de la instalación, la administración del sistema y la configuración de componentes especiales. Además aprenderá los fundamentos teóricos de algunas particularidades de Linux, y en especial de SuSE Linux. Puede encontrar, por ejemplo, información general acerca del sistema X Window, del concepto de arranque, de la impresión o del kernel de Linux.

El trabajo con redes sigue siendo uno de los puntos fuertes de Linux. De ahí que se dedique una gran parte del manual a la teoría, la configuración y la administración de redes con sus distintos protocolos y servicios. Encontrará una gran cantidad de información sobre protocolos, enrutadores, NFS y NIS, así como sobre redes heterogéneas con Samba y Netatalk, y sobre proxies. En la parte final se recoge un detallado capítulo sobre el tema de la seguridad en redes.

Descubrirá que SuSE Linux es sencillamente el mejor sistema operativo se mire por donde se mire, desde la idea del movimiento Open Source hasta el concepto de arranque y la sencillez de la instalación, pasando por el funcionamiento estable y seguro en red o la extremada flexibilidad del entorno X11.

Las versiones digitales de ambos manuales SuSE Linux están disponibles en el sistema instalado en la sección SuSE Linux de la Ayuda de SuSE.

Novedades del Manual de Administración

En este apartado encontrará un listado de los cambios que se han realizado en la documentación de la actual versión respecto a la anterior:

- El capítulo dedicado a Kerberos ha sido completado en cuanto a la instalación y configuración (véase la sección *Instalación y administración de Kerberos* en la página 515).
- Se ha añadido información sobre la gestión de energía ("powermanagement") en la sección *APM y ACPI – Powermanagement* en la página 230.
- Puede encontrar instrucciones para configurar el editor Emacs en el apartado *Configuración de GNU Emacs* en la página 272.
- Muchas otras secciones del manual han sido actualizadas para adaptarlas a las novedades de SuSE Linux 8.2.
- Se ha eliminado el capítulo sobre la configuración de YaST. La información ha sido trasladada al *Manual de Usuario* o a los capítulos correspondientes del *Manual de Administración* en el caso de temas específicos.
- Los siguientes capítulos son totalmente nuevos:
 - Un capítulo sobre las listas de control de acceso (*Access Control Lists*) en Linux B en la página 559.
 - Información sobre "smpppd" en la sección *smpppd como asistente para la conexión telefónica* en la página 470.
 - Información sobre la instalación de parches RPM en el apartado *RPM y parches* en la página 57.
 - Una nueva sección sobre la sincronización de ficheros en el apartado *Sincronización de ficheros* en la página 427.

Convenciones tipográficas

En este manual se utilizan las siguientes convenciones tipográficas:

Convención	Significado
YqST	indica el nombre de un programa
/etc/passwd	indica un fichero o un directorio
⟨fichero⟩	una sucesión de signos fichero que debe ser sustituida por el valor correspondiente (incluidos los paréntesis)
PATH	una variable de entorno con el nombre PATH
192.168.1.2	el valor de una variable
ls	indica el comando que se debe introducir
usuario	indica un usuario
Alt	tecla para pulsar; si están separadas por espacios en blanco se deben pulsar una detrás de otra
Control + Alt + Supr	separadas por el signo '+' se deben pulsar simultáneamente
"Permission denied"	mensajes del sistema
'Actualizar sistema'	la opción de menú 'Actualizar sistema'
"modo DMA"	convenciones de nombres y definiciones

Agradecimientos

La lista de todas las personas que han contribuido al éxito de esta distribución llenaría por sí sola todo un libro. Por tanto, agradecemos conjuntamente a todos aquellos que han aportado un esfuerzo infatigable, grandes cantidades de café y de tabaco, incontables horas extra y noches sin dormir, por haber conseguido una vez más una excelente distribución de SuSE Linux que supera a todas las anteriores.

Los desarrolladores de Linux han hecho posible que Linux se convierta en una realidad gracias a su trabajo voluntario y conjunto en todo el mundo. Les damos

las gracias por su dedicación, sin la cual no sería posible esta distribución. También nos gustaría darles las gracias a Frank Zappa y Pawar.

Por último -pero no por eso menos importante- nuestro agradecimiento especial a Linus Torvalds.

Have a lot of fun!

Su equipo SuSE

Parte I

Instalación

La instalación

SuSE Linux puede instalarse de forma flexible atendiendo a las necesidades individuales; las modalidades varían desde una instalación “rápida” en modo gráfico hasta una instalación en modo texto donde se permite la interacción manual.

A continuación encontrará información sobre la distintas opciones de instalación, como p. ej. la instalación en modo texto con YaST o el uso de diferentes medios de instalación (CD-ROM, NFS). La descripción detallada de la instalación gráfica estándar se encuentra al principio del manual del usuario. En este capítulo se incluyen consejos respecto a problemas en la instalación así como instrucciones para solucionarlos. Al final del capítulo encontrará una sección que describe en detalle el proceso de particionamiento.

Instalación en modo texto con YaST	8
Iniciar SuSE Linux	16
Instalaciones especiales	18
Consejos y trucos	21
Particionar para usuarios avanzados	26
Configuración de LVM con YaST	31
Gestor de volúmenes lógicos (LVM)	32
Soft-RAID	39

Atención

En este manual de administración solamente puede encontrar opciones especiales de instalación. La descripción detallada de la instalación gráfica estándar se encuentra al inicio del manual del usuario.

Atención

Instalación en modo texto con YaST

Información adicional

Además de la instalación con interfaz gráfica también existe la posibilidad de instalar SuSE Linux mediante los menús de texto de YaST (modo de consola). Todos los módulos YaST se encuentran disponibles también en modo texto. El modo texto se puede emplear sobre todo si no existe necesidad de un entorno gráfico (sistemas de servidor) o si la tarjeta gráfica no está soportada por el sistema X Window. Las personas ciegas que no pueden prescindir de una interfaz textual por supuesto también emplearán este modo texto.

La pantalla de bienvenida

Introduzca el CD1 en el dispositivo correspondiente y reinicie el ordenador. Si éste no arranca, es posible que tenga que cambiar el orden de arranque del ordenador en la BIOS a CDR0M, C, A.

Al cabo de unos instantes aparece la pantalla de bienvenida. Tiene 10 segundos para elegir 'Manual Installation' con las teclas $\uparrow$ y $\downarrow$ para que YaST *no* arranque automáticamente. Indique en la línea `boot options` los parámetros de arranque que su hardware pudiera requerir. Normalmente no es necesario indicar parámetros especiales. Con el parámetro `textmode=1` puede hacer que YaST utilice toda la pantalla en modo texto. A la hora de introducir texto, tenga en cuenta que en esta fase del proceso de arranque estará trabajando con un teclado norteamericano.

Las teclas F2 a F5 le permiten definir la resolución de la pantalla para la instalación. Si lo desea, pulse F2=texto para cambiar al modo de sólo texto y después $\downarrow$.

Ahora aparece una ventana con una indicación de progreso "Loading Linux kernel"; después arranca el kernel y se inicia `linuxrc`.

El programa `linuxrc` está basado en menús y espera las indicaciones del usuario.

Posibles problemas

- El resto de problemas durante el arranque suelen poder evitarse con parámetros del kernel. Para aquellos casos en los que DMA sea causa de problemas, se ofrece la opción de inicio ‘Installation - Safe Settings’.
- Si su unidad de CD-ROM (ATAPI) se cuelga al arrancar el sistema, consulte por favor el apartado *Un lector CD-ROM ATAPI se traba leyendo* en la página 25.
- El CD1, que contiene un kernel optimizado para procesadores Pentium, no se reconoce como medio de arranque. Intente usar como alternativa el “disquete de arranque” o el CD2 (ver apartados *Arrancar con un disquete (SYSLINUX)* en la página 23 y *Arrancar con el CD 2* en la página 24).
- En caso de dificultades con ACPI (ingl. *Advanced Configuration and Power Interface*), puede utilizar los siguientes parámetros del kernel:

acpi=off Este parámetro apaga completamente el sistema ACPI. Esta opción puede resultar útil en caso de que su ordenador no disponga de soporte ACPI o si usted cree que la implementación de ACPI es fuente de problemas.

acpi=oldboot Apaga el sistema ACPI casi por completo y sólo utiliza los elementos necesarios para el arranque.

acpi=force Activa ACPI incluso si su ordenador está equipado con un BIOS anterior a 2000. Este parámetro sobrescribe **acpi=off**.

pci=noacpi Este parámetro apaga el PCI IRQ-Routing de sistemas ACPI nuevos.

- Con tarjetas gráficas como FireGL 1, 2 o 3 no se puede arrancar en modo gráfico. En este caso hay que realizar la instalación en modo texto. Por lo tanto, seleccione (**F2=Text**) en el menú de arranque.
- Escoja la opción ‘Memory Test’, para comprobar el estado de la memoria, cuando aparezcan problemas “imprevistos” al cargar el kernel o durante la instalación. ¡Linux plantea grandes exigencias al hardware y a la memoria, por lo que el timing debe configurarse sin ningún fallo! Más información en:

http://sdb.suse.de/en/sdb/html/thallma_memtest86.html

Se recomienda realizar la prueba de memoria por la noche.

La base: linuxrc

Con el programa linuxrc puede realizar ajustes para la instalación, y cargar los controladores que necesite como módulos de kernel. Al final linuxrc arrancará el programa de instalación YaST y puede comenzar la verdadera instalación del software de sistema y de las aplicaciones.

Con $\uparrow$ y $\downarrow$ se selecciona un punto de menú, y con $\leftarrow$ y $\rightarrow$ se selecciona un comando como 'Aceptar' o 'Cancelar'. Con $\downarrow$ se ejecuta el comando. Una descripción detallada de linuxrc se encuentra en el apartado [linuxrc](#) en la página 278.

Configuración

El programa linuxrc se inicia automáticamente con la selección del idioma y de la distribución del teclado.



Figura 1.1: Selección del idioma

- Elija un idioma para la instalación (p. ej. 'Español') y confirme con $\downarrow$.
- Seleccione la distribución del teclado (p. ej. 'Español').

Posibles problemas

- linuxrc no ofrece la distribución del teclado deseada. En este caso seleccione primero una distribución alternativa (en caso de dudas ‘English (US)’; después de la instalación puede cambiar a la distribución exacta mediante YaST).

Menú principal de linuxrc

Ahora nos encontramos en el menú principal de linuxrc (figura 1.2).



Figura 1.2: Menú principal de linuxrc

Aquí hay las siguientes opciones:

‘Configuración’ Aquí puede adaptar el idioma, la pantalla o el teclado. Esto ya lo hemos hecho.

‘Información del sistema’ En este punto hay gran cantidad de información sobre el hardware, siempre que éste haya sido detectado por el kernel o accedido por módulos ya cargados.

‘Módulos del Kernel (Driver)’ Aquí debe cargar los módulos adecuados para su hardware. Además es posible optar por un sistema de archivos alternativo como ReiserFS.

Por regla general *no* es necesario elegir este punto de menú si tanto los discos duros como la unidad de CD (ATAPI) están conectados a una controladora (E)IDE, ya que el soporte para (E)IDE está integrado en el kernel. Puede encontrar más información sobre la selección de módulos en la siguiente sección.

‘Iniciar la instalación / Sistema’ Aquí se pasa a la verdadera instalación.

‘Salir/Reiniciar’ Por si ha cambiado de idea...

‘Apagar’ Para parar y apagar el sistema.

La integración de hardware mediante módulos

La carga de módulos adicionales mediante la opción ‘Módulos de kernel (Drivers)’, se requiere para habilitar características especiales del sistema, como el soporte para SCSI, tarjetas red o PCMCIA o en caso de *no* tener un lector de CDs tipo ATAPI. Últimamente también se han modularizado componentes como IDE y añadido otros nuevos como p. ej. USB, FireWire o sistemas de ficheros.

La carga de módulos se explica en el apartado [linuxrc](#) en la página 278. En el siguiente sub-menú se indica la razón por la que se deben cargar los módulos. Existen las siguientes posibilidades:

Un módulo SCSI Para un disco duro SCSI o un lector CD-ROM de este tipo.

Un módulo CD-ROM Si el lector CD-ROM *no* está conectado a la controladora (E)IDE ni a la controladora SCSI. Esto afecta sobre todo a unidades antiguas de CD-ROM conectadas al ordenador a través de una controladora propietaria.

Un módulo de red En el caso de que se realice la instalación a través de NFS o FTP – lo cual no se trata en este apartado, sino en el apartado [Instalación desde una fuente en la "red"](#) en la página 18.

Uno o varios sistemas de ficheros p. ej. ReiserFS o ext3.

Truco

Si no se encuentra soporte para el medio de instalación usado (Tarjeta PCMCIA, tarjeta de red, lector CD-ROM en controladora propia o en puerto paralelo) dentro de los módulos estándar, se puede recurrir a los drivers adicionales de un disquete de módulos. La creación de tal disquete está explicado [Crear un disquete de arranque bajo DOS](#) en la página 21. Diríjase al final de la lista, y seleccione allí la opción ‘-- Otros módulos --’; `linuxrc` pide en este caso el disquete de módulos.

Truco

Iniciar instalación

Como generalmente ya está seleccionado ‘Iniciar la instalación / Sistema’, sólo tiene que pulsar  para llegar a la auténtica instalación.

Aquí puede elegir entre los siguientes puntos:

‘Comenzar la instalación/actualización’ Supuestamente la opción que elegirá ahora.



Figura 1.3: Menú de instalación de linuxrc

‘Iniciar el sistema instalado’ Puede recurrir a este punto más adelante si se presentan problemas con el cargador de arranque.

‘Iniciar sistema de rescate’ Aquí puede iniciar un sistema de rescate que le ayudará en caso de problemas serios con el sistema instalado.

‘Expulsar CD’ Expulsar el CD de la unidad de CD.

Para llegar a la instalación pulse ahora **(Intro)** con el punto de menú ‘Comenzar la instalación/actualización’ seleccionado. Después tiene que elegir el medio fuente; generalmente no hace falta hacer más que dejar el cursor en la preselección: ‘CD-ROM’.

Pulse ahora **(↵)**. Se inicia el entorno de instalación directamente del CD 1.

En cuanto haya terminado este proceso se inicia YaST en la versión de interfaz textual (ncurses). Después, respecto al contenido, la instalación continúa como se describe en *?, capítulo Instalación*.

Posibles problemas

- No se detecta la controladora SCSI conectada:
 - Intente cargar el módulo de un controlador compatible.



Figura 1.4: Selección del medio fuente linuxrc

- Emplee un kernel que tenga integrado el controlador SCSI correspondiente. Un kernel de estas características debe ser creado por usted.
- La unidad de CD (ATAPI) se cuelga al leer: ver apartado [Un lector CD-ROM ATAPI se traba leyendo](#) en la página 25
- En ciertas circunstancias pueden ocurrir problemas al cargar los datos al disco RAM, dando como resultado que no se pueda cargar YaST. En la mayoría de los casos con el procedimiento siguiente se obtiene una configuración que se pueda usar:

Seleccione en el menú 'Configuración' del menú principal de linuxrc → 'Debug (expertos)'; allí elija 'Cargar imagen raíz (rootimage)' (ingl. *force root image*) y responda no. Vuelva al menú principal y vuelva a comenzar la instalación.

Iniciar SuSE Linux

Una vez completada la instalación, sólo queda decidir cómo quiere arrancar Linux en el día a día (Arrancar).

A continuación le ofrecemos un resumen de las distintas alternativas para iniciar Linux. La decisión de cuál de estos métodos de inicio es el más adecuado para usted, depende sobre todo del propósito previsto.

Disquete de arranque Para arrancar Linux con el *disquete de arranque*. Esta posibilidad siempre funciona y no representa ningún trabajo. El disquete de arranque puede generarse con Yast; véase ?, capítulo *Yast- Configuración*, sección *Crear un disco de arranque, rescate o módulos*.

El disquete es una buena solución intermedia si no se tiene en el momento otra posibilidad o si se prefiere postergar la decisión sobre este tema. También en combinación con OS/2 o Windows NT, el uso del disquete de arranque puede representar una solución.

Linux Bootloader La solución más limpia desde un punto de vista técnico y más universal, es el uso de un gestor de arranque de Linux, como GRUB (GRand Unified Bootloader) o LILO (LIinux LOader), que permiten seleccionar entre distintos sistemas operativos antes de arrancar. El gestor de arranque se puede instalar directamente durante la primera instalación de sistema o bien más tarde, p. ej. mediante Yast.

Aviso

Hay determinadas versiones de BIOS que comprueban la estructura del sector de arranque (MBR) y que emiten – por equivocación – la advertencia de presencia de virus después de la instalación de GRUB o LILO. Lo más sencillo para resolverlo es entrar en la BIOS y tratar de desactivar la protección antivirus ('Virus Protection'). – Una vez que Linux esté instalado es posible activar esta característica de nuevo, pero si se usa el ordenador exclusivamente con Linux tampoco hace falta.

Aviso

Se puede encontrar una amplia explicación sobre los diferentes métodos de arranque y en especial sobre GRUB y LILO en el capítulo 4 en la página 73 ff.

La pantalla gráfica de SuSE

Desde la versión SuSE Linux 7.2 aparece una pantalla gráfica con el logo de SuSE en la consola 1, si como parámetro del kernel se ha activado la opción

"vga=<valor>". En la instalación con YAST esta opción es anotada automáticamente en correspondencia con la resolución seleccionada y la tarjeta gráfica empleada.

Desactivar la pantalla de SuSE

En principio existen tres diferentes posibilidades:

- Desactivar la pantalla especial bajo demanda.

Para realizarlo se ha de teclear en la línea de comandos

```
tierra:~ # echo 0 >/proc/splash
```

Con el siguiente comando

```
tierra:~ # echo 0x0f01 >/proc/splash
```

se enciende la pantalla gráfica nuevamente.

- Desactivar la pantalla de SuSE definitivamente:

Para realizarlo se ha de añadir el parámetro de kernel `splash=0` a la configuración del gestor de arranque. En el capítulo [El proceso de arranque y el gestor de arranque](#) en la página 73 encontrará más información.

Para trabajar en el modo texto habitual de las versiones anteriores de SuSE Linux se puede escribir `"vga=normal"`.

- Desactivar la pantalla SuSE "para siempre":

Esta desactivación se realiza compilando un kernel nuevo. En la configuración del kernel se ha de desactivar la opción dentro del menú 'framebuffer support'.

Truco

Al desactivar el soporte de framebuffer dentro del kernel, el "Splash-Screen" se desactiva automáticamente. ¡SuSE no ofrece ningún soporte en caso de haber compilado un kernel propio!

Truco

Instalaciones especiales

Instalación sin lector CD-ROM soportado

¿Qué hacer si no es posible efectuar una instalación estándar a través de un lector CD-ROM? El lector CD-ROM podría ser uno de los modelos "propietarios" antiguos para los que no siempre existe soporte. También es posible que no se tenga una unidad CD-ROM en un segundo ordenador (p. ej. un portátil) pero que sí se tenga una tarjeta Ethernet.

SuSE Linux ofrece también la posibilidad de instalar el sistema en un ordenador sin soporte CD-ROM pero con una conexión de red Ethernet. En estos casos se suele utilizar NFS o FTP vía Ethernet, que será lo que se describa a continuación.

Instalación desde una fuente en la "red"

El soporte no cubre esta vía de instalación, por lo que sólo los usuarios experimentados deberían usar este método.

Para instalar SuSE Linux a través de una fuente en la red, son necesarios dos pasos:

1. Depositar los datos necesarios para la instalación (CDs, DVD) en un ordenador que actuará posteriormente como fuente de la instalación.
2. Arrancar el sistema que se va a instalar con un disquete o CD y configurar la red.

Crear una fuente de instalación en la red

Para crear la autorización de acceso a la red, copie los CDs de instalación a directorios individuales y guarde éstos en un sistema con prestaciones de servidor NFS. Por ejemplo, puede utilizar el siguiente comando para copiar cada CD en un ordenador con SuSE Linux:

```
tierra:/ # cp -a /mnt/cdrom /suse-share/
```

Después cambie el nombre del directorio (por ejemplo a "CD1"):

```
tierra:/ # mv /suse-share/cdrom /suse-share/CD1
```

Repita este procedimiento para el resto de CDs. Finalmente, liberalice el directorio /suse-share mediante NFS ; véase la sección *NFS – Sistema de archivos distribuidos* en la página [382](#).

Arrancar para instalar a través de la red

Introduzca el medio de arranque en la unidad correspondiente. En las secciones *Crear un disquete de arranque bajo DOS* en la página 21 y *Crear un disquete de arranque bajo un sistema tipo Unix* en la página 22 se describe cómo crear un disquete de arranque. Poco después aparecerá el menú de arranque. Seleccione aquí la entrada 'Instalación Manual'. En este punto también puede añadir parámetros para la instalación. Confirme la selección con (Intro). El kernel se cargará y se le pedirá que introduzca el primer disquete de módulos.

A continuación aparece linuxrc y tendrá que definir algunos parámetros:

1. Seleccione el idioma y la distribución del teclado en linuxrc.
2. Seleccione 'Módulos del kernel (controladores de hardware)'.
3. Si su sistema lo requiere, cargue los controladores IDE, RAID o SCSI necesarios.
4. Seleccione 'Cargar controlador de red' y cargue el controlador de red necesario en su caso (p. ej. `eeepro100`).
5. Seleccione 'Cargar controlador para el sistema de archivos' y cargue el controlador requerido (p. ej. `reiserfs`).
6. Seleccione 'Atrás' y a continuación 'Iniciar instalación / sistema'.
7. Seleccione 'Iniciar instalación / actualización'.
8. Seleccione 'Red' y NFS como protocolo de red.
9. Seleccione la tarjeta de red que quiere utilizar.
10. Introduzca las direcciones IP y la información adicional de red.
11. Introduzca la dirección IP del servidor NFS que proporciona los datos para la instalación.
12. Introduzca la ruta al recurso compartido NFS (p. ej. `/suse - share/CD1`).

linuxrc carga de la fuente de red el entorno de instalación y a continuación inicia YaST.

Finalice la instalación como se describe en ?, Capítulo *Instalación*.

Posibles problemas

- La instalación termina antes de haber comenzado realmente: El directorio de instalación del "otro" ordenador no se ha sido exportado con derechos de ejecución (exec) – modifíquelo.
- El servidor desconoce en qué ordenador se ha de instalar SuSE Linux. Introduzca en el archivo `/etc/hosts` del servidor, el nombre y la dirección IP del nuevo ordenador.

Consejos y trucos

Crear un disquete de arranque bajo DOS

Requisitos

Se necesita un disquete HD de 3.5 pulgadas formateado y la disquetera correspondiente que permita el arranque.

Información adicional

En el directorio `boot` del CD 1 se encuentran algunas representaciones o imágenes (images) de disquetes (images). Estas imágenes pueden copiarse en disquetes utilizando los programas de ayuda adecuados. Las disquetes pasan a llamarse entonces disquetes de arranque. Estas imágenes de disquete contienen también el "Loader" Syslinux y el programa `linuxrc`. El programa Syslinux permite seleccionar un kernel durante el arranque y pasar parámetros al hardware. El programa `linuxrc` presta asistencia cuando se cargan módulos del kernel especiales para el hardware y finalmente inicia la instalación.

Procedimiento

Para crear los disquetes de arranque y de los módulos se usa el programa DOS `rawrite.exe` (CD 1, `\dosutils\rawrite`). Para esto se necesita un ordenador con DOS (p. ej. FreeDOS) o Windows instalado.

A continuación se describen los pasos que tiene que seguir si trabaja con Windows:

1. Introduzca el CD 1 de SuSE Linux.
2. Abra una ventana de DOS (en el menú Start bajo 'Programas' → 'MS-DOS Prompt').
3. Ejecute el programa `rawrite.exe` con la ruta correcta del lector de CD. En el siguiente ejemplo Usted se encuentra en el disco duro `C:`, en el directorio `Windows` y el lector de CD tiene asignada la letra `D:`.

```
C:\Windows> d:\dosutils\rawrite\rawrite
```

4. Después de arrancar, el programa solicita el tipo de fuente (ingl. *source*) y el destino (ingl. *destination*) del archivo a copiar. En nuestro ejemplo se trata del disquete de arranque que pertenece a nuestro juego de CDs cuya imagen se encuentra en el CD 1 en el directorio `\boot`.

El nombre de archivo es sencillamente `bootdisk`. No olvide indicar aquí también la ruta del lector de CD.

```
C:\Windows> d:\dosutils\rawrite\rawrite
RaWrite 1.2 - Write disk file to raw floppy diskette
Enter source file name: d:\boot\bootdisk
Enter destination drive: a:
```

Después de indicar como destino `a:` `rawrite` le solicita introducir un disquete formateado y pulsar `(Enter)`. A continuación se muestra el progreso del proceso de copiar. Es posible interrumpir la acción pulsando `(Control) + (C)`.

De la misma manera puede crear los otros disquetes `modules1`, `modules2`, `modules3` y `modules4`. Los necesita si tiene dispositivos SCSI, USB, una tarjeta de red o una tarjeta PCMCIA, y quiere acceder a éstos durante el proceso de instalación. El disquete de módulos puede resultar también muy útil si quiere utilizar un sistema de archivos especial ya durante la instalación.

Crear un disquete de arranque bajo un sistema tipo Unix

Requisitos

Dispone de un sistema Linux o tipo Unix equipado con un lector CD-ROM; además se necesita un disquete libre de errores (formateado).

Para crear el disquete de arranque se procede de la siguiente manera:

1. Si aún falta formatear el disquete:

```
tierra:~ # fdformat /dev/fd0u1440
```

2. Montar el primer CD (Disk 1); p. ej. hacia `/cdrom`:

```
tierra:~ # mount -tiso9660 /dev/cdrom /cdrom
```

3. Cambiar al directorio `boot` en el CD:

```
tierra:~ # cd /cdrom/disks
```

4. Generar el disquete de arranque con:

```
tierra:~ # dd if=/cdrom/disks/bootdisk of=/dev/fd0 bs=8k
```

En el archivo `README` en el directorio `boot` puede encontrar más información sobre las imágenes de disquetes. Puede visualizar este archivo con `more` o `less`.

De la misma manera puede crear los otros disquetes `modules1`, `modules2`, `modules3` y `modules4`. Los necesita si tiene dispositivos SCSI, USB, una tarjeta red o PCMCIA y quiere acceder a estos durante el proceso de instalación. El disquete de módulos puede resultar también muy útil si quiere utilizar un sistema de archivos especial durante la instalación.

El asunto se complica un poco si durante la instalación se quiere utilizar un kernel que ha compilado usted mismo. En este caso se copia primero la imagen estándar (`bootdisk`) en el disquete y se sobrescribe el kernel del disquete (`linux`) con el kernel propio (véase el apartado [Compilación del kernel](#) en la página 262):

```
tierra:~ # dd if=/media/cdrom/boot/bootdisk of=/dev/fd0 bs=8k
tierra:~ # mount -t msdos /dev/fd0 /mnt
tierra:~ # cp /usr/src/linux/arch/i386/boot/vmlinuz /mnt/linux
tierra:~ # umount /mnt
```

Arrancar con un disquete (SYSLINUX)

El “disquete de arranque” puede utilizarse siempre que existan requisitos especiales a la hora de realizar la instalación (p. ej. unidad de CD-ROM no disponible). Para ver cómo se crea un disquete de arranque, consulte las secciones [Crear un disquete de arranque bajo DOS](#) en la página 21 o [Crear un disquete de arranque bajo un sistema tipo Unix](#) en la página anterior.

El proceso de arranque es iniciado por el cargador de arranque SYSLINUX (paquete `syslinux`). SYSLINUX está configurado de tal modo que durante el arranque se lleva a cabo una pequeña detección de hardware. Esta consta básicamente de los siguientes pasos:

- Comprobar si la BIOS soporta un framebuffer adecuado para VESA 2.0 y si el kernel puede arrancarse en consecuencia.
- Evaluar los datos del monitor (información DDC).
- Se lee el primer bloque del primer disco duro (“MBR”) para definir posteriormente la asignación de BIOS IDs a los nombres de dispositivos Linux (ingl. *devices*) durante la configuración de LILO. Durante este procedimiento se intenta leer el bloque a través de las funciones `lba32` de la BIOS para ver si la BIOS soporta estas funciones.

Truco

Si la tecla **(Mayús)** o **(Shift)** está pulsada durante el inicio de SYSLINUX, se saltará estos pasos.

Para facilitar la búsqueda de errores es posible insertar la línea
`verbose 1`

en el archivo `syslinux.cfg`. De esta forma el cargador de arranque siempre informa sobre qué acción se va a llevar a cabo a continuación.

Truco

Posibles problemas

- Si el ordenador no quiere arrancar desde el disquete, puede que tenga que cambiar previamente el orden de arranque en la BIOS a A, C, CDROM.

Arrancar con el CD 2

Además de con el CD 1, también es posible arrancar con el segundo CD. Mientras que el CD 1 trabaja con una imagen ISO arrancable, el CD 2 arranca mediante una imagen de disco de 2,88 MB.

Utilice el CD 2 en aquellos casos en los que sabe que, aunque se puede arrancar desde un CD, no es posible hacerlo con el CD 1 (solución alternativa o "fall-back").

¿Soporta Linux mi lector CD-ROM?

Se puede decir que, por lo general, Linux soporta la mayoría de los lectores CD-ROM.

- No se debe presentar ningún problema usando lectores del tipo ATAPI.
- En el caso de lectores tipo SCSI sólo importa que la controladora SCSI, que lleva la conexión al CD-ROM, sea soportada por Linux. Hay una lista de controladoras soportadas en la base de datos de componentes CDB (<http://cdb.suse.de/>). Si no encuentra soporte para su controladora SCSI y el disco duro está conectado a la misma, entonces tiene un problema ...

- También hay muchos lectores CD-ROM propietarios que funcionan con Linux. No obstante, pueden presentarse problemas con este grupo de dispositivos. Si no se menciona explícitamente su lector, se puede probar con uno similar del mismo fabricante.
- Los lectores CD-ROM USB también están soportados. Si la BIOS de su ordenador todavía no soporta el arranque de dispositivos USB, debe iniciar la instalación a través de un disquete de arranque. Puede encontrar más información al respecto en la sección [Arrancar con un disquete \(SYSLINUX\)](#) en la página 23. Antes de arrancar desde el disquete, asegúrese de que los dispositivos USB están conectados y encendidos.

Un lector CD-ROM ATAPI se traba leyendo

Cuando no se reconoce bien un lector CD-ROM ATAPI o él mismo se traba leyendo, en muchos casos se debe a un fallo en la configuración de los componentes. Normalmente todos los dispositivos que se conectan al bus (E)IDE deben estar conectados en fila, es decir, que el primer dispositivo es el master en el primer canal y el segundo es el esclavo. El tercer dispositivo debe ser entonces master en el segundo canal y el cuarto allí el esclavo.

En realidad resulta que muchos ordenadores solamente contienen un disco duro y un CD-ROM que se encuentra entonces como master en el segundo canal. En algunas ocasiones Linux no maneja bien este *vacío*. Muchas veces se puede ayudar al kernel introduciendo un parámetro adicional (`hdc=cdrom`).

También puede ocurrir que un dispositivo tenga los "jumpers" mal colocados; esto quiere decir que está configurado como esclavo pero se encuentra como master en el segundo canal o viceversa. En caso de duda es recomendable comprobar y eventualmente corregir estas configuraciones.

Aparte de esto, hay una serie de "chipsets" EIDE defectuosos que en gran parte ya se conocen y el kernel contiene código para solventar los problemas. Existe un kernel especial para estos casos (ver el README en /boot del CD-ROM de instalación).

Si no se puede arrancar en un principio, se puede probar con los siguientes parámetros del kernel:

hd(x)=cdrom (x) simboliza a, b, c, d etc. y tiene el siguiente significado:

- a – Maestro en la 1ª controladora IDE
- b – Esclavo en la 1ª controladora IDE
- c – Maestro en la 2ª controladora IDE

- ...

Ejemplo para *⟨Parámetro a introducir⟩*: `hdb=cdrom`

Con este parámetro se puede indicar al kernel donde está el lector CD-ROM del tipo ATAPI, si es que el kernel no lo encuentra por sí mismo.

ide⟨x⟩=noautotune *⟨x⟩* simboliza 0, 1, 2, 3 etc. y tiene el siguiente significado:

- 0 – 1ª controladora IDE
- 1 – 2ª controladora IDE
- ...

Ejemplo para *⟨Parámetro a introducir⟩*: `ide0=noautotune`

Este parámetro ayuda normalmente en combinación con discos duros del tipo (E)IDE.

Particionar para usuarios avanzados

En el capítulo de instalación estándar (véase ?) se ha comentado brevemente cómo particionar el sistema. El presente apartado quiere proporcionar información detallada con la cual se pueda crear un esquema de partición optimizado para el sistema. Es además especialmente interesante para aquellos que quieran configurar el sistema de manera óptima, respecto a seguridad y velocidad y que están – según las circunstancias – dispuestos a crear todo desde cero. ¡Arrasar con todo, esa es la idea!

Es fundamental entender el modo de funcionar de un sistema de archivos UNIX. En particular, los conceptos del punto de montaje (Mountpoint) tal como los de las particiones lógicas y extendidas, se deben haber entendido.

Al principio es importante destacar que no existe *un solo* camino óptimo para todos pero que sí existen muchos caminos buenos para cada uno. No hay de qué preocuparse, ya que también habrá reglas y cifras concretas en este apartado.

Como primer paso, se debe reunir la siguiente información:

- ¿Para qué usará su máquina (servidor de archivos, servidor de aplicaciones Compute-Server, estación de trabajo)?
- ¿Cuántas personas trabajarán en el ordenador (contado en logins simultáneos)?
- ¿Cuántos discos duros tiene el ordenador, qué tamaño tienen y qué tipo de interfaz (EIDE, SCSI o una controladora RAID)?

El tamaño de la partición de intercambio (swap)

Todavía se puede leer en muchas partes: "La cantidad de Swap debe ser como mínimo el doble de la de RAM". Esta regla pertenece a la época en la cual 8 MB de RAM eran suficiente. Estos tiempos han pasado. La persona que compra hoy en día un ordenador con menos de 64 MB ha sido muy mal aconsejada. Volviendo a la regla anterior: El fin era conseguir un ordenador con cerca de 30 a 40 MB de Memoria virtual, es decir, de RAM más swap.

Con las aplicaciones modernas, hambrientas de memoria, hay que corregir estos valores hacia arriba. Normalmente 128 MB de memoria virtual es suficiente, pero es mejor no ser tacaño a este respecto. Si se compila el kernel en el entorno KDE y se miran las páginas de ayuda con Netscape mientras que en algún lugar se ejecuta Emacs, con 128 MB de memoria virtual no se dispone de muchas reservas.

Esto significa que al usuario normal le bastará con 256 MB de memoria virtual a medio plazo. Lo que no se debería hacer, bajo ningún pretexto, es no proporcionar ningún tipo de memoria swap. Incluso una máquina con 256 MB RAM debería tener una zona de swap. No obstante, es suficiente con 64 MB de memoria swap para cubrir las necesidades básicas. La razón para ello se detalla en el apartado *Tasa de transferencia a discos y tamaño de memoria* en la página 31.

En el caso de que ejecute simulaciones con gasto de *memoria* del orden de gigabytes, puede que necesite mucha memoria swap. Si se tienen dudas acerca de si Linux puede soportar o no semejante carga, se aconseja leer el apartado *Uso como servidor* en la página 29 (tipo de uso: Compute-Server).

Formas de uso del ordenador

Como estación de trabajo autónoma

Este es el tipo de uso más frecuente de un ordenador con Linux. Para poder orientarse con valores concretos, hemos compilado un par de configuraciones de ejemplo, que pueden ser usadas según sea necesario, en casa o en la empresa. Los espacios requeridos para un determinado tipo de instalación se encuentran en la tabla 1.1 en la página siguiente

Naturalmente estos valores se incrementan si se quiere guardar archivos adicionales, aparte de los propios del sistema.

Estación de trabajo estándar (muy pequeña)

Le sobra un disco duro de alrededor de 500 MB y lo quiere usar para Linux. En este caso genere una partición de intercambio (swap) de 64 MB y reserve el resto para la partición root /.

Instalación	espacio necesario en disco
muy pequeña	180 MB hasta 400 MB
pequeña	400 MB hasta 1500 MB
mediana	1500 MB hasta 4 GB
grande	más de 4 GB

Cuadro 1.1: Ejemplos de tamaños de instalación

Estación de trabajo estándar (promedio)

Le quedan 1,5 GB libres para Linux. Genere una partición de arranque pequeña /boot (5-10 MB o un cilindro), 128 MB para el swap, 800 MB para / y el resto para una partición /home aparte.

Estación de trabajo (lujo)

Si tiene 1,5 GB o incluso más en varios discos, entonces no existe ninguna forma estándar de particionar. A este respecto consulte el apartado *Posibilidades de optimización* en la página siguiente.

Como servidor de archivos

Aquí todo depende *realmente* de las prestaciones del disco duro. En todo caso, son preferibles los discos duros tipo SCSI. También vale la pena tener en cuenta la potencia del disco (SCSI, SCSI Ultra Wide, revoluciones, etc.) y de la controladora. Un servidor de archivos ofrece la posibilidad de almacenar datos de manera centralizada. Se puede tratar de directorio de usuario (directorios de usuario), de una base de datos o de otros archivos diversos. La ventaja es básicamente una administración simplificada. Si el servidor de archivos debe trabajar en una red amplia (a partir de 20 usuarios) la optimización del acceso al disco es esencial.

Supongamos que se quiere configurar un servidor de archivos de base Linux para servir con los directorios personales a 25 usuarios. Se calcula que cada usuario ocupará un máximo de 100-150 MB para sus datos personales. Una partición de 4 GB para montar /home es suficiente, suponiendo que los usuarios no siempre compilan en su directorio personal (home). Con 50 usuarios, el simple cálculo indica que es suficiente con una partición de 8 GB. En realidad resulta mejor montar /home en dos discos de 4 GB, porque éstos se distribuyen entre sí la carga y el tiempo de acceso.

Truco

¡La memoria intermedia (caché) de un navegador web se debe encontrar sobre un disco duro local!

Truco**Uso como servidor**

Un servidor (Compute-Server) es generalmente un ordenador potente que se encarga de tareas de cálculo grandes en una red. Típicamente una máquina de estas características tiene mucha memoria (a partir de 512 MB). El cuello de botella se encuentra aquí, en las particiones de swap. En este caso también cuenta que es mejor distribuir varias particiones swap en varios discos.

Posibilidades de optimización

Generalmente los discos duros son el factor limitador. Existen tres posibilidades diferentes (que se deben usar juntas) para pasar por ese cuello de botella:

- Distribuir la carga de manera equilibrada entre varios discos.
- Utilizar un sistema de archivos optimizado (p. ej. `reiserfs`).
- Equipar el servidor de archivos con suficiente memoria (mínimo 256 MB).

Paralelizar con varios discos

Hay que explicar el primer método con más detenimiento. El tiempo total que transcurre hasta que se pueden proporcionar los datos pedidos a un disco, se constituye (aproximadamente) de las siguientes fases:

1. tiempo, hasta que el pedido está en la controladora.
2. tiempo, hasta que la controladora envíe este pedido al disco duro.
3. tiempo, hasta que el disco duro posiciona su cabezal.
4. tiempo, hasta que el disco se haya girado hacia al sector correcto.
5. tiempo para la transmisión de los datos.

El punto 1 depende de la conexión a la red, se regula allí y no nos debe ocupar ahora. El tiempo mencionado en el punto 2 es muy corto y depende de la controladora misma. Los puntos 3 y 4 suelen ser los más espinosos, ya que se trata de un tiempo que se mide en ms. Comparado con los tiempos de acceso a la memoria RAM, que son del orden de ns, hablamos de un factor de 1 millón(!). El punto 4 depende de las revoluciones del disco y suele sumar varios ms. El punto 5 de esas revoluciones y de la cantidad y posición actual de los cabezales (en la zona interior o exterior del disco).

Lo mejor para un buen rendimiento es entonces "atacar" en el punto 3. Los discos del tipo SCSI lo tratan de mejorar mediante la característica "disconnect". Esta característica significa más o menos lo siguiente: La controladora envía al dispositivo conectado (en este caso el disco duro) la orden "¡Vete a la pista x, sector y!". Ahora la mecánica del disco duro con toda su inercia se tiene que poner en marcha. Si el disco es inteligente (o maneja "disconnect") y el driver de la controladora también conoce esta característica, entonces la controladora del disco envía inmediatamente la orden "disconnect" y el disco se separa del bus SCSI. A partir de ahora, otros dispositivos SCSI pueden llevar a cabo la transferencia de datos. Después de un rato (dependiendo de la estrategia o de la carga en el bus SCSI), se reanuda la conexión al disco duro. En el caso ideal, éste ya habrá llegado con su cabezal a la posición de lectura deseada.

En un sistema multitarea y multiusuario como Linux, quedan muchas posibilidades para optimizar. Se puede observar entonces el resultado de la salida del comando `df` (ver la salida en pantalla 1).

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda5	1.8G	1.6G	201M	89%	/
/dev/sda1	23M	3.9M	17M	18%	/boot
/dev/sdb1	2.9G	2.1G	677M	76%	/usr
/dev/sdc1	1.9G	958M	941M	51%	/usr/lib
shmfs	185M	0	184M	0%	/dev/shm

Mensaje en pantalla 1: Salida de ejemplo del comando `df`

¿Qué ventaja proporciona esta paralelización? Supongamos que se introduce en `/usr/src` lo siguiente:

```
root@tierra:/usr/src/ > tar xzf package.tar.gz -C /usr/lib
```

De este modo se instala `package.tar.gz` en `/usr/lib/package`. Para ello, la shell invoca los programas `tar` y `gzip` (se encuentran en `/bin` y por lo tanto sobre `/dev/sda`), después se lee `package.tar.gz` desde `/usr/src` (se encuentra sobre `/dev/sdb`). Por último, los datos extraídos se escriben en `/usr/lib`, que se encuentra sobre `/dev/sdc`. Ahora el posicionamiento tal como la lectura/escritura de los búferes internos del disco, se pueden llevar a cabo de manera casi paralela.

Lo arriba expuesto es solamente un ejemplo entre muchos. Por experiencia se puede decir que `/usr` y `/usr/lib` se deben encontrar en diferentes discos si se trata de un sistema de varios discos igual de rápidos. La ruta `/usr/lib` debe tener cerca del 70 % de la capacidad de `/usr`. Por la gran cantidad de accesos es conveniente que el directorio `root` se encuentre en el disco con `/usr/lib`.

A partir de una cierta cantidad de discos SCSI (de 4 a 5), conviene considerar seriamente una solución RAID por software o (mejor) la adquisición de una controladora RAID. Con ella, las operaciones en los discos se ejecutarán no solo de manera casi-paralela sino realmente de forma paralela. La tolerancia respecto a fallos es otra agradable ventaja de la tecnología RAID.

Tasa de transferencia a discos y tamaño de memoria

Mencionamos en varios sitios que bajo Linux, el tamaño de la memoria puede resultar en muchas ocasiones más importante que la propia velocidad del procesador. Una razón – sino la *mayor* – es la propiedad que tiene Linux de generar búferes dinámicos con datos del disco duro. Haciendo esto, Linux usa muchos trucos sofisticados como “read ahead” (saca sectores adicionales del disco como provisión para el futuro) y “delayed write” (ahorra grabar datos para luego guardar una mayor cantidad de información de una sola vez). Esto último es la razón por la cual no se puede simplemente apagar un ordenador con Linux. Ambos trucos son los responsables del hecho que la memoria aparezca con el tiempo más llena y de que Linux sea tan rápido.; ver también apartado *El comando free* en la página 271

Configuración de LVM con YaST

Con esta herramienta de particionamiento para expertos podrá editar particiones ya existentes, borrarlas o crear nuevas particiones. También la ofrece la posibilidad de configurar un Soft-RAID o LVM.

Atención

Puede encontrar información más detallada y consejos para particionar en el capítulo *Particionar para usuarios avanzados* en la página 26.

Atención

Aunque todas las particiones se configuran durante la instalación, si desea añadir un disco duro tendrá que particionar primero el disco nuevo, formatear y montar las particiones para posteriormente darles de alta en `/etc/fstab`. Es posible que sea necesario mover algunos datos al disco nuevo, p. ej. para mover una partición `/opt` demasiado pequeña al nuevo disco.

Hay que tener mucho cuidado al reparticionar el disco duro con el que se está trabajando en ese momento. Aunque en principio es posible, es necesario arrancar el sistema inmediatamente después de realizarlo, por lo que arrancar desde CD y reparticionar conlleva mucho menos riesgo.

El botón ‘Opciones Experto’ dentro del particionador abre un menú con las siguientes opciones:

Reset and Re-Read Leer nuevamente las particiones del disco duro. Se necesita p. ej. en caso de haber particionado en la consola de texto.

Read old fstab Se utiliza sólo durante la instalación. Leer la `fstab` antigua sirve para instalar el sistema nuevamente en lugar de actualizarlo. Leyendo la `fstab` antigua no hace falta introducir los puntos de anclaje manualmente.

Delete old Partition Table Borrar la tabla de particiones completamente. Puede ser útil en caso de tener p. ej. problemas con ciertos formatos de disco extraños; todos los datos en el disco duro se pierden.

Gestor de volúmenes lógicos (LVM)

El gestor de volúmenes lógicos (ingl. *Logical Volume Manager (LVM)*) permite distribuir el espacio del disco de forma flexible en diferentes sistemas de archivos. El LVM se desarrolló por la dificultad que supone modificar las particiones en un sistema en ejecución. LVM pone en común un depósito o “pool” virtual (Volume Group – abreviado VG) de espacio en disco. De este VG se forman los volúmenes lógicos en caso necesario. El sistema operativo accede entonces a éstos en lugar de acceder a las particiones físicas.

Particularidades:

- Es posible juntar varias particiones o discos para formar una gran partición lógica.
- Si un LV se queda (p. ej. /usr) sin espacio, es posible aumentar su tamaño si está correctamente configurado.
- LVM permite añadir discos duros o LV incluso cuando el sistema está en marcha. Esto requiere, evidentemente, hardware que se pueda cambiar en caliente (hot swap).
- Es posible utilizar varios discos duros en modo RAID 0 (striping) con el consiguiente incremento de rendimiento.
- La función "snapshot" permite, sobre todo en servidores, realizar copias de seguridad coherentes mientras el sistema está en funcionamiento.

El uso de LVM vale la pena ya a partir de PCs domésticos muy utilizados o en servidores pequeños. LVM resulta ideal para un volumen de datos creciente como p. ej. en el caso de bases de datos, colecciones de MP3, directorios de usuarios, etc. En tal caso es posible configurar sistemas de archivos más grandes que un solo disco duro. Otra ventaja del LVM es la de poder crear hasta 256 LVs. Sin embargo, es importante considerar que el trabajo con el LVM se diferencia mucho del trabajo con particiones convencionales.

Puede encontrar información en inglés sobre la configuración del gestor de volúmenes lógicos en el HowTo oficial de LVM o en un white paper de SuSE:

- <http://www.sistina.com/lvm/Pages/howto.html>
- <http://www.suse.com/us/support/oracle/>

Configurar el LVM con YaST

La configuración del LVM mediante YaST se activa seleccionando 'Particionar con LVM' en el primer paso de la preparación del disco duro durante la instalación. En la siguiente pantalla, haga clic en 'Desechar' o en 'Modificar', tras lo cual debe crear una partición para LVM. Para ello, elija 'Crear' → 'No formatear' y allí escoja el punto '0X8e Linux LVM'. Puede realizar la partición con LVM directamente o más tarde sobre el sistema instalado, para lo cual deberá marcar la partición LVM en el particionador y luego pulsar en 'LVM...'.

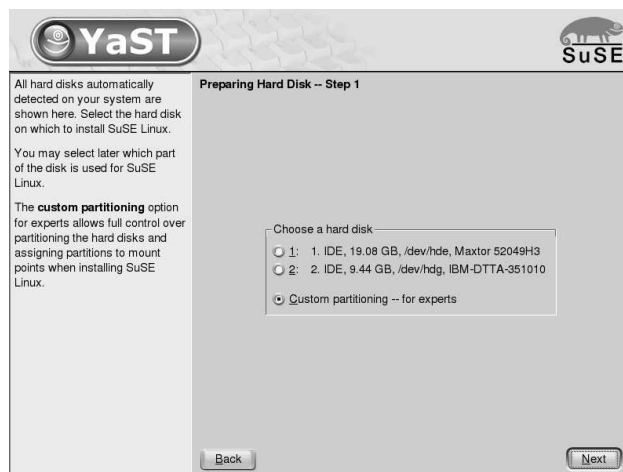


Figura 1.5: YaST: Activar LVM durante la instalación

LVM – Particionador

Tras haber escogido ‘LVM...’ en el particionador, aparecerá un primer diálogo en el que puede modificar las particiones de su disco duro; le permite borrar o modificar particiones existentes, así como crear otras nuevas. Las particiones que formarán parte del LVM debe llevar el indicador 8E y estar marcadas con el texto “Linux LVM” en de la lista de particiones (ver último apartado).

Truco

Reparticionar volúmenes lógicos

Al principio de los volúmenes físicos o PVs, se escribe información sobre el volumen en la partición. De esta forma, el PV “sabe” a qué grupo de volumen pertenece. Si desea volver a particionar, se recomienda borrar el inicio de estos volúmenes. Por ejemplo, en el caso de un grupo de volumen “system” y un volumen físico “/dev/sda2”, esto se realiza con el comando `dd if=/dev/zero of=/dev/sda2 bs=512 count=1`

Truco

No hace falta que configure uno por uno el indicador 8E para todas las particiones que compondrán el LVM, ya que YaST se ocupa de modificar el indicador de una partición integrante de un grupo de volúmenes cuando es necesario.

Si hay espacios sin particionar en el disco duro, es recomendable crear particiones LVM para todas estas zonas y asignarles inmediatamente el indicador 8E.

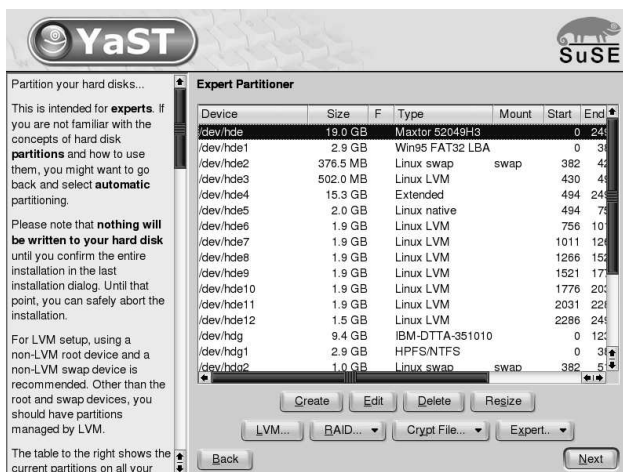


Figura 1.6: YaST: Particionador LVM

Estas particiones no tienen que ser formateadas y no se puede indicar ningún punto de anclaje para ellas.

Si tuviera instalado un LVM válido en la máquina, éste se activaría automáticamente al comienzo de la configuración de LVM. Después de esta activación ya no se pueden modificar las particiones de ningún disco duro que albergue una partición integrante de un grupo de volúmenes (VG) activado. El kernel de Linux deniega el permiso para leer la tabla de particiones modificada de un disco duro mientras alguna partición de este disco esté en uso.

Aquellos discos que no forman parte de un grupo de volúmenes LVM se pueden reparticionar sin problemas, pero al disponer ya de una configuración válida de LVM, normalmente no hace falta cambiar las particiones. En la pantalla actual debe configurar todos los puntos de anclaje que no estén vinculados al LVM. YaST pide que al menos el sistema de archivos raíz se encuentre sobre una partición normal. Seleccione esta partición de la lista y utilice 'Editar' para definirla como sistema de archivos raíz (ingl. *root file system*). Debido a la mayor flexibilidad de LVM, recomendamos ubicar los demás sistemas de archivos sobre volúmenes lógicos. – Una vez definida la partición raíz, puede salir del diálogo.

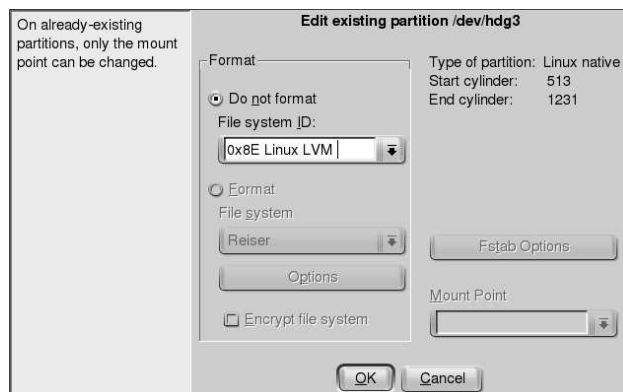


Figura 1.7: YaST: Crear partición LVM

LVM – Configuración de los volúmenes físicos

En el diálogo 'LVM' se administran los grupos de volúmenes LVM (abreviados como VG). Si aún no se ha creado ningún VG aparecerá una ventana que pide su creación. La propuesta para el nombre del VG que albergará los datos del sistema SuSE Linux es el nombre `system`.

El valor "Physical Extent Size" (abreviado PE size) determina el tamaño máximo de un volumen físico y lógico dentro del grupo de volúmenes. Este valor se sitúa normalmente en 4 megabytes y permite 256 gigabytes como tamaño máximo para un volumen físico y lógico. No aumente el PE size (p. ej. a 8, 16 ó 32 megabytes), si no necesita volúmenes lógicos más grandes de 256 gigabytes.

La siguiente ventana muestra todas las particiones de los tipos "Linux LVM" o "Linux native" (no se muestra ninguna partición DOS o de intercambio (swap)). En el caso de las particiones que ya forman parte del grupo de volúmenes, la lista muestra el nombre del grupo de volúmenes al que pertenecen. Las particiones no asignadas están marcadas con "--".

Se puede cambiar el grupo de volúmenes sobre el que se trabaja en la ventana de selección que se encuentra en la parte superior izquierda. Con los botones de la parte superior derecha se pueden crear nuevos grupos de volúmenes y eliminar los ya existentes. Sin embargo, sólo se pueden eliminar los VGs que no estén asignados a ninguna partición. Para un sistema SuSE Linux normal no es necesario crear más de un grupo de volúmenes. Una partición asignada a un VG se denomina volumen físico (ingl. *Physical Volume* o PV).

Para añadir una partición aún no asignada al grupo de volúmenes seleccionado, se debe elegir primero la partición y pulsar después el botón 'Añadir volumen'.

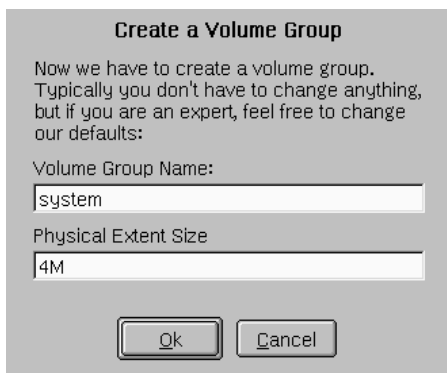


Figura 1.8: YaST: Crear un grupo de volúmenes

debajo de la lista de particiones. El nombre del grupo de volúmenes aparecerá entonces junto a la partición seleccionada. Todas las particiones previstas para LVM deben ser asignadas a un grupo de volúmenes para aprovechar todo el espacio en el disco. No se puede salir del diálogo antes de haber asignado al menos un volumen físico a cada grupo de volúmenes.

Volúmenes lógicos

Este diálogo permite administrar los volúmenes lógicos (ingl. *Logical Volumes* o *LV*)

Los volúmenes lógicos siempre están asignados a un grupo de volúmenes y tienen un determinado tamaño. Si desea crear un RAID 0 durante la creación del volumen lógico, ha de crear en primer lugar el LV con un número mayor de bandas ("stripes"). Un LV con n bandas sólo puede crearse correctamente cuando el espacio de disco requerido por LV puede distribuirse de forma uniforme en n volúmenes físicos. Si sólo están disponibles dos PVs, un LV con 3 bandas no sería viable.

Sobre un volumen lógico se crea normalmente un sistema de archivos (p. ej. `reiserfs`, `ext2`) y se asigna un punto de anclaje al volumen. Éste es el punto de acceso para llegar posteriormente a los datos que se guardan sobre este volumen lógico. La lista muestra todas las particiones normales de Linux que ya tienen un punto de anclaje asignado, todas las particiones de swap y todos los volúmenes lógicos ya existentes. A los volúmenes lógicos ya existentes en el sistema hace falta asignarles un punto de anclaje. Al configurar LVM por primera vez, aún no existen volúmenes lógicos en la lista y es necesario crear un volumen lógico

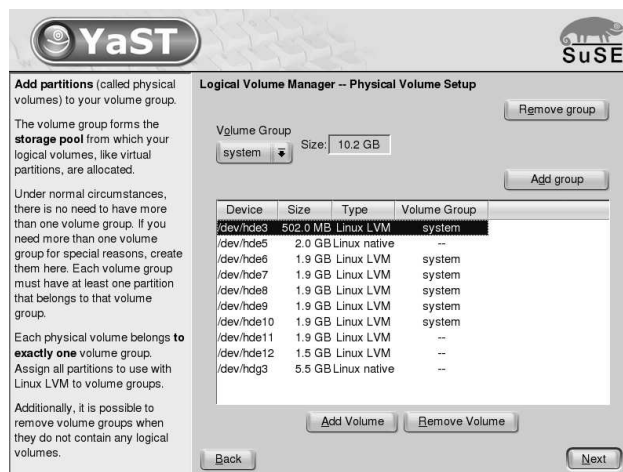


Figura 1.9: YaST: Resumen de las particiones

para cada punto de anclaje. Esto se lleva a cabo con el botón 'Añadir', indicando el tamaño, el tipo de sistema de archivos (p. ej. reiserfs o ext2) y el punto de anclaje (p. ej. /var, /usr, /home).

En caso de haber creado varios grupos de volúmenes, es posible cambiar entre los diferentes grupos de volúmenes con la lista de selección en la parte superior izquierda. Todos los volúmenes lógicos creados se encuentran en el grupo mostrado en el recuadro. Una vez que todos los volúmenes lógicos se hayan configurado correctamente, la configuración de LVM finaliza. Ahora ya puede salir de este apartado y, si se encuentra dentro de la instalación de sistema, continuar con la selección de software.

Aviso

La configuración del LVM puede implicar riesgos como p. ej. la pérdida de datos. Algunos de los peligros potenciales son la caída de programas, los cortes de suministro eléctrico o los comandos equivocados.

Por eso es importante realizar copias de seguridad de los datos antes de configurar el LVM o antes de modificar volúmenes. ¡Nunca se debe trabajar sin una copia de seguridad!

Aviso

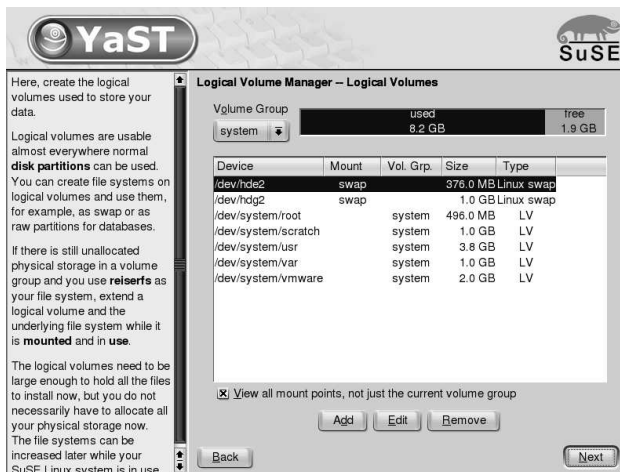


Figura 1.10: YaST: Administración de volúmenes lógicos

Soft-RAID

La idea de un RAID (ingl. *Redundant Array of Inexpensive Disks*) es el de juntar varias particiones para formar un disco duro "virtual" grande y así optimizar el rendimiento o la seguridad de los datos. El "RAID-Level" determina la forma de unir y de acceder a los discos duros que se conectan a una controladora RAID. Estas controladoras suelen emplear el protocolo SCSI ya que éste es capaz de controlar más discos duros de una forma más eficiente que el protocolo IDE. Además ofrece ventajas respecto al tratamiento de comandos en paralelo.

En lugar de una controladora RAID, que puede resultar muy costosa, el Soft-RAID es también capaz de encargarse de estas tareas. SuSE Linux ofrece la posibilidad de unir mediante YaST varios discos duros en un Soft-RAID. Es una alternativa muy económica al hardware RAID.

Niveles de RAID habituales

RAID 0 Este nivel mejora la velocidad de acceso a los datos. En realidad no se trata de un RAID porque no existe ninguna seguridad de datos pero la denominación "RAID 0" se ha hecho habitual para esta constelación con al menos dos discos duros. El rendimiento es muy alto, pero todo el sistema RAID se estropea al dañarse un solo disco y todos los datos se pierden.

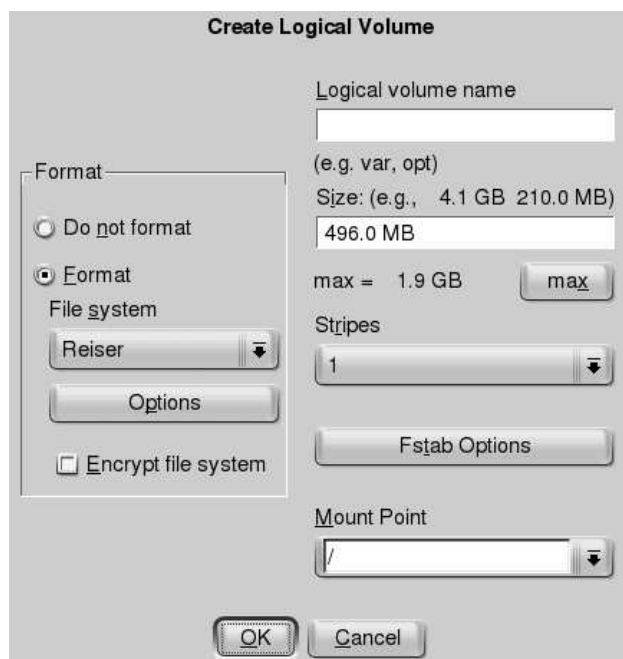


Figura 1.11: YaST: Crear volúmenes lógicos

RAID 1 Este nivel ofrece una seguridad aceptable de los datos, porque se encuentran copiados con exactitud en otro disco duro. La constelación se denomina "Mirroring" o "Mirror" de disco; también es usual hablar de discos "espejados". Esto quiere decir que existe una duplicación simultánea de los datos en uno o varios discos. Cuando un disco se estropea existe una copia en otro, así que se pueden romper todos los discos a excepción de uno sin perder datos. La velocidad de escritura baja del 10 al 20 % por la necesidad de escribir los datos en más de un disco, pero la velocidad de lectura es bastante más alta porque los datos se pueden leer simultáneamente en varios discos.

RAID 5 RAID 5 es el resultado optimizado de los dos anteriores niveles de RAID en cuanto al rendimiento y la seguridad de datos. La capacidad de almacenamiento del RAID equivale a la capacidad total de los discos duros menos uno; es decir, los datos se distribuyen igual que en el caso de RAID 0 sobre todos los discos y la seguridad de los datos está dada por la información de paridad que se encuentra, en el caso de RAID 5,

sobre uno de los discos. Estos “bloques de paridad” se enlazan mediante un XOR lógico para conseguir la recuperación de una partición después de su rotura. En el caso de RAID 5 nunca se debe estropear más de un disco duro en el mismo momento para no perder información. Por eso es importante reemplazar un disco duro dañado lo más rápidamente posible.

Configurar un Soft-RAID con YaST

Se puede acceder a la configuración del Soft-RAID mediante la opción ‘RAID’ dentro de ‘Sistema’ o a través del módulo de particionar en ‘Hardware’.

Paso 1: Particionar

La primera pantalla de la ‘Configuración avanzada’ de la herramienta de particionar muestra todas las particiones existentes. Si ya ha creado particiones para el Soft-Raid, éstas aparecerán dentro de la lista. En caso contrario se han de crear particiones nuevas. RAID 0 y RAID 1 requieren al menos de dos particiones – para RAID 1 suelen ser exactamente dos. RAID 5 en cambio necesita al menos tres particiones. Las particiones deben tener el mismo tamaño y se deben encontrar sobre diferentes discos duros para suprimir el riesgo de pérdida de datos por daño de un disco para RAID 1 y 5 o para aumentar el rendimiento en caso de RAID 0.

Paso 2: Crear el RAID

Pulsando sobre ‘RAID’ aparece el diálogo para seleccionar el nivel de RAID (0,1 o 5). La siguiente pantalla permite asignar las particiones al RAID nuevo. Las ‘Opciones avanzadas’ permiten ajustar la configuración con más detalle, como la modificación del “chunk-size” para aumentar la eficiencia del RAID. Al marcar la casilla ‘Superbloque persistente’, las particiones RAID se reconocen como tales directamente al arrancar el ordenador.

Después de haber terminado la configuración aparecerá el dispositivo `/dev/md0` marcado como RAID dentro del apartado experto en el módulo de particionar.

Resolución de problemas

El contenido del archivo `/proc/mdstats` informa sobre daños en una partición RAID. En caso de daños hay que parar el sistema Linux y reemplazar el disco dañado por uno equivalente y con las mismas particiones. Después se puede reiniciar el sistema y ejecutar el comando `raidhotadd /dev/mdX /dev/sdX`, que automáticamente integra el disco duro nuevo en el RAID y lo reconstruye.

Puede encontrar una introducción a la configuración de Soft Raid así como información adicional (en inglés) en los siguientes Howto:

- [/usr/share/doc/packages/raidtools/Software-RAID-HOWTO.html](#)
- <http://en.tldp.org/HOWTO/Software-RAID-HOWTO.html>

o en la lista de correo de Linux RAID p. ej. en

- <http://www.mail-archive.com/linux-raid@vger.rutgers.edu>

en la que puede encontrar también ayuda para problemas más complejos.

Actualización del sistema – Gestión de paquetes

SuSE Linux ofrece la posibilidad de actualizar un sistema existente sin necesidad de instalar todo desde cero. Hay que distinguir entre la *actualización de algunos paquetes* y la *actualización del sistema completo*.

Paquetes particulares También se puede instalar manualmente con el gestor de paquetes rpm.

Actualización de SuSE Linux	44
Cambio del software de una versión a otra	49
RPM – El gestor de paquetes	54

Actualización de SuSE Linux

Es un fenómeno conocido, el hecho de que el software "crezca" de versión en versión, por lo que se recomienda averiguar de cuánto espacio se dispone en las particiones, usando `df`, *antes* de la actualización. Si se tiene la impresión de estar un poco "justo" de espacio, se recomienda hacer una copia de seguridad de los datos antes de empezar con la actualización y modificar las particiones (aumentar su tamaño). Es difícil determinar la cantidad de espacio necesario ya que éste depende en gran medida de las particiones actuales, del software elegido y desde qué versión se va a realizar la actualización.

Atención

Para obtener información sobre cambios o suplementos *posteriores* a la impresión de este libro, se puede consultar el archivo `README` o bajo DOS/Windows el archivo `README.DOS` – ambos se encuentran en el CD.

Atención

Preparativos

Antes de realizar cualquier actualización se deben copiar los archivos de configuración a un medio independiente (cinta, disquetes, unidad-ZIP, etc.); sobre todo se trata de los archivos contenidos en `/etc` pero también se debe tener en cuenta el directorio `/var/lib`. Además se deben respaldar los datos actuales de los usuarios en `/home`; son los directorios `HOME`. Esta copia de seguridad se debe efectuar como Administrador de sistema (`root`) ya que sólo `root` tiene los derechos de lectura de todos los archivos locales.

Antes de comenzar con la actualización se debe anotar el nombre de la partición raíz que se obtiene con el comando `df /`. En el caso de la salida en pantalla 2, `/dev/hda7` es la partición raíz que se debe anotar, ya que es ésta la que está montada bajo `/`.

Filesystem	Size	Used	Avail	Use%	Mounted on
<code>/dev/hda1</code>	1.9G	189M	1.7G	10%	<code>/dos</code>
<code>/dev/hda7</code>	3.0G	1.1G	1.7G	38%	<code>/</code>
<code>/dev/hda5</code>	15M	2.4M	12M	17%	<code>/boot</code>
<code>shmfs</code>	141M	0	141M	0%	<code>/dev/shm</code>

Mensaje en pantalla 2: Resumen con `df -h`

Posibles problemas

PostgreSQL Antes de actualizar PostgreSQL (paquete `postgres`), se deben volcar (ingl. *dump*) todas las bases de datos al disco; ver página del manual de `pg_dump` (`man pg_dump`). Evidentemente esto solo es necesario si se ha usado PostgreSQL antes de la actualización.

Controladora Promise Hoy en día en diversos ordenadores se encuentran las controladoras IDE de la empresa Promise, en placas base de alta calidad. Algunas veces como controladoras puras de IDE (para UDMA 100) y otras como controladoras IDE-RAID. A partir de SuSE Linux 8.0 hay soporte directo del kernel para estas controladoras y las trata como si fueran controladoras normales para discos duros IDE. Sólo el módulo del kernel `pdraid` habilita la funcionalidad RAID.

Al actualizar puede ocurrir en algunos casos que se detecta discos duros conectados a la controladora de Promise antes de los discos duros en la controladora normal de IDE. En este caso el sistema no arrancará después de una actualización del kernel y típicamente se despedirá con "Kernel panic: VFS unable to mount root fs". Para arreglarlo al arrancar se debe indicar el parámetro de kernel `ide=reverse` para invertir el orden de la detección de los discos duros; ver apartado [La pantalla de bienvenida](#) en la página 8. Use YOST para introducir este parámetro de forma duradera en la configuración de arranque; ver el capítulo *La instalación del usuario, Arrancar (Instalación del gestor de arranque)* en el *YaST2, Modo de arranque* en el manual ?

Aviso

Sólo se pueden encontrar las controladoras que estén activadas en la BIOS. La activación o desactivación anterior o posterior de las controladoras en la BIOS tiene una influencia directa en la denominación de los dispositivos. ¡Proceder de forma desconsiderada puede tener como consecuencia la imposibilidad de arrancar el sistema!

Aviso

Explicación técnica

El orden de las controladoras depende de la placa base. Cada fabricante tiene su propia estrategia de integrar controladoras adicionales. Mediante el comando `lspci` se puede visualizar la orden. Si se lista la controladora Promise como controladora IDE normal hay que indicar, después de actualizar el parámetro de kernel, `ide=reverse`. El kernel viejo (sin soporte directo para Promise) ignoraba la controladora y detectaba primero la controladora IDE normal.

El primer disco duro era entonces `/dev/hda`. Con el nuevo kernel se detecta directamente la controladora Promise y por consiguiente sus discos duros (hasta cuatro) con `/dev/hda`, `/dev/hda`, `/dev/hdb`, `/dev/hdc` y `/dev/hdd`. El hasta ahora disco `/dev/hda` se convierte de repente en `/dev/hde` y en consecuencia no se encuentra en el proceso de arranque.

Actualización con YaST

Después de los preparativos del apartado *Preparativos* en la página 44, inicie el proceso de arranque.

1. Inicie el sistema como para la instalación (véase el manual de usuario) y, después de seleccionar el idioma, *no* elija en YaST ‘Nueva instalación’, sino ‘Actualizar un sistema ya existente’.
2. YaST determinará si existe más de una partición raíz. En caso negativo, pase a la sección 3. En caso de que existan varias particiones, seleccione la partición correcta y confirme con ‘Siguiendo’. En el ejemplo de la sección *Preparativos* en la página 44 seleccionó `/dev/hda7`.

YaST también lee el “antiguo” `fstab` que se encuentra en esta partición para analizar y a continuación montar los sistemas de archivos allí existentes.

3. Posteriormente existe la posibilidad de crear una copia de seguridad de los archivos del sistema durante la actualización. Aunque esta opción ralentiza el proceso de actualización, debe seleccionarse si no dispone de una copia de seguridad actual del sistema.
4. En el siguiente diálogo se puede decidir si sólo se debe actualizar el software instalado o si se deben añadir al sistema nuevos componentes de software importantes (“modo upgrade”). Se recomienda aceptar la combinación predeterminada (por ejemplo ‘sistema estándar’). Si existe alguna discrepancia, se puede eliminar posteriormente con YaST.

Actualización manual

Actualización del sistema base

Al actualizar el sistema base se cambian los componentes centrales del sistema (p. ej. las bibliotecas), por lo tanto esto no se puede llevar a cabo desde el sistema Linux en ejecución.

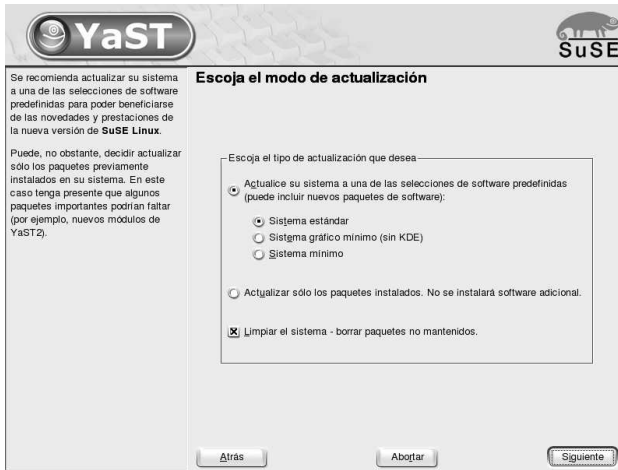


Figura 2.1: Actualización del sistema

Por esta razón se tendrá que arrancar el entorno de actualización. Esto se hace normalmente bien con el CD, con el DVD o con el disquete de arranque ("Boot-disk" que se ha creado anteriormente). Si quiere efectuar intervenciones manuales o realizar la actualización entera con el "ncurses-ui" de YaST (modo texto), hay que seguir esencialmente los pasos que ya se han descrito detalladamente en el apartado *Instalación en modo texto con YaST* en la página 8:

Básicamente hay que seguir los pasos que se exponen a continuación:

1. Inmediatamente después del arranque del sistema, desde el disquete de arranque o desde el CD o bien DVD, se inicia automáticamente linuxrc.
2. linuxrc pide escoger en la opción 'Configuración' del menú principal, el idioma y el teclado (siempre se confirma pulsando 'Ok').
3. Con la opción 'Módulos del Kernel (Drivers)' se cargan los drivers necesarios para el hardware. El procedimiento se detalla en el apartado *La base: linuxrc* en la página 10 y en la descripción de linuxrc, en la página 280.
4. Ahora se puede elegir el medio fuente de la instalación pasando por las opciones 'Iniciar la instalación / Sistema' → 'Comenzar la instalación' (ver en la página 282).
5. linuxrc carga el entorno de instalación proporcionado por YaST, tal como se ha elegido.

En el primer menú de YqST, seleccione – después de haber elegido el idioma – la opción ‘Actualizar sistema’. A continuación YqST intenta detectar la partición raíz y ofrece varias posibilidades de las cuales se debe seleccionar la partición raíz, tal como se ha anotado anteriormente (ejemplo: /dev/sda3). YqST lee la /etc/fstab “antigua” que se encuentra sobre esta partición, y monta los sistemas de archivos anotados en ella.

Después existe la posibilidad de realizar una copia de seguridad de los archivos del sistema durante la actualización.

En el diálogo siguiente puede definir que solo se actualice el software ya instalado o bien que se añadan nuevos e importantes componentes de software al sistema. Se recomienda aceptar la composición propuesta (p. ej. ‘Sistema predefinido’). Con YqST se pueden eliminar eventuales divergencias.

Diálogo de advertencia: ‘Sí - instalar’ para que pueda realizarse la transferencia del nuevo software desde el medio fuente al disco duro del sistema.

Revisión de la base de datos RPM

A continuación se actualizan los componentes centrales del sistema y YqST genera automáticamente copias de seguridad de los archivos modificados a partir de la última instalación; además, los archivos de configuración antiguos se guardan con la extensión .rpmorig o .rpmsave (ver el apartado *Instalar, actualizar y desinstalar paquetes* en la página 56). Todo el proceso de instalación y actualización se protocoliza en el archivo /var/adm/inst-log/installation- *.

Actualización del resto de programas

Una vez instalado el sistema base, se entra al modo especial de actualización de YqST que permite actualizar el resto del sistema según necesidades y/o preferencias.

Después de haber seleccionado los paquetes, el proceso se termina como una instalación desde cero; entre otras cosas, se tendrá que seleccionar también un kernel nuevo.

Truco

Si está acostumbrado a iniciar Linux con loadlin, es preciso copiar el *nuevo* kernel – y si es el caso – el *initrd* en el directorio de loadlin de la partición DOS!

Truco

Posibles problemas

- En caso de que el entorno shell no se comporte del modo esperado, revise los archivos de su home que comienzan con un punto y compruebe que todavía son adecuados para su sistema. Si no es así coja por favor las versiones actuales de `/etc/skel`; p. ej.:

```
cp /etc/skel/.profile ~/.profile
```

Actualización de paquetes individuales

Independientemente de la actualización del sistema base, se pueden actualizar paquetes sueltos en cualquier momento. Realizando una actualización parcial, el *usuario mismo* se tiene que encargar de mantener la consistencia del sistema en cuanto a las dependencias de los paquetes. Consejos sobre la actualización se encuentran bajo <http://www.suse.de/en/support/download/updates/>

Esto se realiza en YaST entrando al submenú ‘Escoger/Instalar paquetes’. Se puede seleccionar cualquier paquete, pero si selecciona uno que es esencial para el sistema, YaST advierte sobre la necesidad de actualizar tal paquete en el modo especial de actualización. Hay muchos paquetes que usan p. ej. librerías compartidas (ingl. *shared libraries*), que pueden estar en uso en el momento de la actualización y por tanto se podrían producir errores.

Cambio del software de una versión a otra

Los siguientes apartados mencionan los detalles que se han cambiado de una versión de SuSE Linux a otra, como por ejemplo el cambio de lugar de un archivo de configuración o una modificación importante de un programa conocido. La lista es incompleta ya que solo se mencionan los aspectos importantes para el trabajo diario de los usuarios o del administrador de sistema. En la descripción de las diferencias y particularidades hay muchas referencias a la base de datos de soporte (SDB) del paquete `sdb_en`.

Los problemas y cambios de última hora de cada versión se publican en nuestro servidor web; véase los links que se indican más abajo. Se puede actualizar determinados paquetes importantes vía <http://www.suse.de/en/support/download/updates/>.

De 7.3 a 8.0

Problemas y Particularidades:

<http://sdb.suse.de/sdb/en/html/bugs80.html>.

- Los disquetes de arranque sólo se distribuyen en forma de imágenes de disquetes (antiguo directorio `disks`, ahora directorio `boot`). Un disquete de arranque se necesita solamente si no es posible arrancar desde CD; dependiendo del hardware y de la intención de la instalación hay que crear adicionalmente disquetes de las imágenes `modules1`, `modules2`, etc. El procedimiento está descrito en *Crear un disquete de arranque bajo DOS* en la página 21 o bien en *Crear un disquete de arranque bajo un sistema tipo Unix* en la página 22.
- YaST2 sustituye por completo a YaST1, también en los modos de texto o consola. Cuando en estas líneas se hable de "YaST", nos estamos refiriendo siempre a la nueva versión.
- Algunas BIOS necesitan el parámetro del kernel `realmode-power-off`; hasta versión 2.4.12 del kernel se llamaba `real-mode-poweroff`
- La variable `START` de `rc.config` para iniciar los servicios ya no es necesaria. Todos los servicios se arrancan si existen los enlaces correspondientes en los directorios de niveles de ejecución o `runlevel`. Los enlaces se crean con `insserv`.
- Los servicios del sistema se configuran mediante variables en los archivos de `/etc/sysconfig`; al actualizar el sistema se toma en consideración las configuraciones de los archivos en `/etc/rc.config.d`.
- Se ha dividido `/etc/init.d/boot` en varios scripts y movido a otros paquetes () en caso oportuno. (ver paquete `kbd`, paquete `isapnp`, paquete `lvm` etc); véase en la página 300.
- En el tema de redes se han realizado una gran cantidad de modificaciones; véase el apartado *El acceso a la red* en la página 326.
- Para la gestión de los archivos de registro (ingl. *logfiles*) se hace use de `logrotate`; `/etc/logfiles` es obsoleto; ver apartado *Archivos de registro – el paquete logrotate* en la página 268.
- Se puede permitir un login de `root` via `telnet` o `rlogin` mediante entradas en los archivos en `/etc/pam.d`. Por razones de seguridad ya no se permite el arranque de `ROOT_LOGIN_REMOTE` con `yes`.

- `PASSWD_USE_CRACKLIB` puede ser activado con `YvST`.
- Cuando se deben compartir archivos NIS para `autofs` via NIS, se debe utilizar el módulo NIS-Client de `YvST` para la configuración. Una vez allí, active ‘Arrancar automontador’. La variable `USE_NIS_FOR_AUTofs` se ha quedado obsoleta.
- `locate` para la búsqueda rápida de archivos ya no forma parte del software instalado por defecto. En caso necesario, instálelo (paquete `find-locate`) y se iniciará como de costumbre automáticamente unos 15 minutos después de haber arrancado el proceso `updatedb`
- El soporte del ratón se encuentra activo para `pine`, lo cual significa que se puede hacer funcionar `Pine` en una `xterm` haciendo clic en una opción del menú. Sin embargo también significa que sólo se puede copiar y pegar pulsando la tecla del tabulador, si el soporte del ratón está activo, lo que no es el caso en una nueva instalación. Al actualizar no se debe descartar que esta opción está activa (si hay un antiguo `~/pinerc` disponible. En este caso, se puede desactivar la opción `enable-mouse-in-xterm` en la configuración de `Pine`, con lo que todo vuelve a la normalidad.

De la 8.0 a la 8.1

Problemas y particularidades:

<http://sdb.suse.de/sdb/de/html/bugs81.html>.

- Modificaciones en los nombres de usuario y grupo del sistema: Para que concuerden en `UnitedLinux` se ajustaron algunas entradas en `/etc/passwd` o `/etc/group`.
 - Usuario modificado: `ftp` se encuentra en el grupo `ftp` (y no en `daemon`).
 - Grupos que han cambiado de nombre: `www` (era `wwwadmin`); `games` (era `game`).
 - Grupos nuevos: `ftp` (con GID 50); `floppy` (con GID 19); `cdrom` (con GID 20); `console` (con GID 21); `utmp` (con GID 22).
- Modificaciones relacionadas con FHS (véase apartado *Filesystem Hierarchy Standard (FHS)* en la página 266):
 - Un entorno de ejemplo para HTTPD (Apache) se encuentra en `/srv/www` (antes era `/usr/local/httpd`).

- Un entorno de ejemplo para FTP se encuentra en `/srv/ftp` (antes era `/usr/local/ftp`). Para ello se requiere el paquete `ftplib`.
- Para facilitar el acceso al software deseado, los paquetes ya no se encuentran en unas pocas y complicadas series, sino en "grupos RPM". La consecuencia de esto es que en los CDs ya no hay directorios codificados bajo `suse`, sino sólo unos pocos directorios denominados en función de la arquitectura, como p. ej. `ppc`, `i586` o `noarch`.
- En una instalación nueva se configuran los siguientes programas, o dicho de otro modo, ya no se instalan automáticamente:
 - El gestor de arranque GRUB, que ofrece más posibilidades que LILO. LILO se mantiene al actualizar un sistema ya existente.
 - El programa de correo postfix en vez de sendmail.
 - En vez de majordomo se instala mailman, el moderno software de listas de correo.
 - ¡`hardened_suse` se debe escoger a mano y leer la documentación al respecto!
- Paquetes divididos: `rpm` en `rpm` y `rpm-devel`; `popt` en `popt` y `popt-devel`; `libz` en `zlib` y `zlib-devel`.
`yast2-trans-*` ahora dividido por idiomas: `yast2-trans-cs` (checo), `yast2-trans-de` (alemán), `yast2-trans-es` (español) etc.; en la instalación ya no se instalan todos los idiomas con el fin de ahorrar espacio en el disco duro. En caso de ser necesario, instale posteriormente el resto de los paquetes con el soporte de idiomas de YaST.
- Paquetes que han cambiado de nombre: `bzip` en `bzip2`.
- Paquetes que no se incluyen: `openldap`, en su lugar utilizar ahora `openldap2`. `su1`: a partir de ahora le rogamos utilizar `sudo`.

De 8.1 a 8.2

Problemas y peculiaridades:

<http://sdb.suse.de/sdb/en/html/bugs82.html>.

- Soporte 3D para tarjetas gráficas basadas en nVidia (cambios): los paquetes RPM `NVIDIA_GLX/NVIDIA_kernel` (incluyendo el script `switch2nvidia_glx`) ya no están incluidos. Descargue el instalador de nVidia para Linux IA32 de la página web de nVidia

(<http://www.nvidia.com>), utilícelo para instalar el controlador y active el soporte 3D por medio de SxX2 o YaST.

- En caso de una nueva instalación, xinetd se instala en vez de inetd y es configurado de forma segura con valores predeterminados (véase el directorio `/etc/xinetd.d`). En caso de una actualización, se mantendrá inetd.
- La versión incluida de PostgreSQL es la 7.3. Si actualiza desde la versión 7.2.x, es necesario realizar un “dump/restore” con el comando `pg_dump`. Si su aplicación consulta los catálogos del sistema debe además realizar modificaciones adicionales, ya que la versión 7.3 incorpora nuevos esquemas. Puede encontrar más información en:
http://www.ca.postgresql.org/docs/momjian/upgrade_tips_7.3
- La versión 4 de stunnel ha dejado de soportar opciones en la línea de comandos. No obstante, se incluye el script `/usr/sbin/stunnel3_wrapper`, el cual es capaz de convertir las opciones de línea de comando en un archivo de configuración adecuado para stunnel y de ejecutar dicho archivo al ejecutar el siguiente comando (sustituya `<OPTIONS>` por las opciones correspondientes):

```
/usr/sbin/stunnel3_wrapper stunnel <OPTIONS>
```

El archivo de configuración creado será mostrado en los datos de salida estándar, de forma que puede utilizar sus entradas para crear un archivo de configuración permanente de cara al futuro.

- `openjade` (paquete `openjade`) es el motor DSSSL que, sustituyendo a `jade` (paquete `jade_dsl`), se activa cuando se inicia `db2x.sh` (paquete `docbook-toys`). Debido a motivos de compatibilidad, los programas también están disponibles sin el prefijo ‘o’.

Para evitar un conflicto con el paquete `paquete rzsx`, la herramienta de la línea de comandos `sx` se sigue llamando `s2x`, `sgml2xml` u `osx`.

De 8.2 a 9.0

Problemas y peculiaridades:

<http://sdb.suse.de/sdb/en/html/bugs90.html>.

- La versión incluida del gestor de paquetes RPM es la 4. La funcionalidad para construir paquetes ha sido transferida al programa independiente `rpmbuild`. `rpm` sigue siendo utilizado para instalar, actualizar y realizar consultas a la base de datos, ver sección 2.
- En la sección *Impresión* se encuentra el paquete `footmatic-filters`. El contenido se ha tomado del paquete `cups-drivers`, ya que la experiencia ha demostrado que es posible imprimir con él aún cuando CUPS no está instalado. De esta forma es posible definir con YaST configuraciones independientes del sistema de impresión (CUPS, LPRng). El archivo de configuración de este paquete es `/etc/foomatic/filter.conf`.
- Para utilizar LPRng/lpfilter se requieren los paquetes `footmatic-filters` y `cups-drivers`.
- Puede accederse a los recursos XML del paquete de software incluido en la distribución a través de entradas en `/etc/xml/suse-catalog.xml`. Este archivo no puede ser editado con `xmlcatalog`, ya que los comentarios organizativos desaparecerán en caso contrario. Estos comentarios son imprescindibles para garantizar que la actualización se lleve a cabo correctamente. El acceso a `/etc/xml/suse-catalog.xml` se realiza a través de una declaración `nextCatalog` en `/etc/xml/catalog`, de tal forma que herramientas XML como `xmllint` o `xsltproc` encuentren automáticamente los recursos locales.

RPM – El gestor de paquetes

SuSE Linux utiliza RPM (ingl. *RPM Package Manager*) con los programas principales `rpm` y `rpmbuild` para la administración de los paquetes de software. La gran base de datos de RPM facilita la gestión de los paquetes para todos los implicados: los usuarios, los administradores de sistema y los que generan los paquetes; RPM ofrece una gran cantidad de información sobre el software instalado.

Básicamente, `rpm` puede actuar de cinco maneras distintas: instalar, desinstalar o actualizar paquetes de software, volver a crear la base de datos RPM, enviar consultas a la base de datos RPM o a archivos RPM individuales, comprobar la integridad de los paquetes y firmar paquetes. `rpmbuild` sirve para generar paquetes listos para instalar a partir de las fuentes originales (ingl. *pristine sources*).

Los archivos RPM, listos para ser instalados tienen un formato binario especial que incluye los archivos con los programas e información adicional usada por `rpm`. Esta información adicional se usa para configurar el software del paquete o

para la documentación en la base de datos RPM. Estos archivos tienen la extensión `.rpm`.

Con `rpm` se pueden gestionar los paquetes LSB; más sobre LSB en el apartado [Linux Standard Base \(LSB\)](#) en la página 266.

Truco

En el caso de varios paquetes, los componentes necesarios para el desarrollo del software (librerías, archivos “header” e “include”) han pasado a ser paquetes separados; se trata de un procedimiento que ya se llevó a cabo en versiones anteriores. Estos paquetes sólo serán necesarios para desarrollos propios; p. ej. compilar paquetes de GNOME más recientes. Este tipo de paquetes se identifica normalmente con el suplemento `-devel` en su nombre; algunos ejemplos son: paquete `alsa-devel`, paquete `gimp-devel`, paquete `kdelibs-devel`, etc.

Truco

Comprobar la autenticidad de un paquete

Los paquetes RPM de SuSE están firmados con GnuPG:

```
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 apache-1.3.12.rpm
```

comprueba la firma de un paquete RPM para averiguar si este realmente fue hecho por SuSE o por otra entidad de confianza; es un procedimiento que se recomienda especialmente con los paquetes de actualización de Internet. Nuestra clave pública para firmar los paquetes se encuentra por defecto en `/root/.gnupg/`. Desde la versión 8.1, esta clave también se incluye en el directorio `/usr/lib/rpm/gnupg/` para que los usuarios normales también puedan comprobar la firma de los paquetes RPM.

Instalar, actualizar y desinstalar paquetes.

Por lo general la instalación de un archivo RPM se realiza rápidamente:

```
rpm -i (paquete).rpm
```

Este comando estándar solamente instala un paquete si se cumplen todas las dependencias, ya que de lo contrario podrían aparecer conflictos; los mensajes de

error de rpm indican los paquetes que faltan para cumplir con las dependencias. La base de datos se ocupa de evitar conflictos: normalmente un archivo debe pertenecer a un solo paquete; también hay diferentes opciones que permiten pasar por alto esta regla, pero se debe estar muy seguro de ello ya que se puede perder la posibilidad de actualizar el paquete.

Algunas opciones muy interesantes para la actualización de un paquete son -U o --upgrade y -F o --freshen.

```
rpm -F <paquete>.rpm
```

Por medio de este comando se borra la antigua versión de un paquete y se instala la nueva. La diferencia entre ambas opciones radica en que en el caso de -U también se instalan paquetes que hasta ahora no estaban disponibles en el sistema, mientras que la opción -F sólo actualiza un paquete que ya estuviera instalado. Por su parte, rpm trata los archivos de configuración con cuidado, apoyándose en la siguiente estrategia:

- Si el administrador de sistema no ha cambiado ningún archivo de configuración, rpm instala la versión nueva y por lo tanto, el administrador de sistema no tiene que intervenir de ninguna manera.
- Si el administrador de sistema ha cambiado un archivo de configuración antes de realizar la actualización, rpm guarda el archivo con la extensión .rpmorig o .rpmsave e instala la nueva versión del paquete RPM, salvo que el archivo de configuración de esta nueva versión no haya cambiado su estructura. En el caso de reemplazar el archivo de configuración, es muy probable que sea necesario adaptar el nuevo basándose en la copia con la extensión .rpmorig o .rpmsave.
- Archivos con extensión .rpmnew siempre aparecen cuando el archivo de configuración ya existe y si el indicador noreplace aparece dentro del archivo .spec.

Después de la actualización se deben borrar los archivos .rpmorig, .rpmsave y .rpmnew para que estos no obstaculicen la siguiente actualización. La extensión .rpmsave se selecciona cuando la base de datos RPM ya conoce el archivo, en caso contrario se usa .rpmorig. Dicho en otras palabras, los ".rpmorig" se generan cuando se actualizan paquetes que no tienen formato RPM y los .rpmsave se generan actualizando paquetes RPM antiguos con RPM nuevos. La extensión .rpmnew se usa cuando no se puede determinar si el administrador de sistema realmente modificó el archivo de configuración o no.

Puede encontrar una lista de estos archivos en /var/adm/rpmconfigcheck.

Compruebe que no se sobrescriben determinados archivos de configuración (p. ej. `/etc/httpd/httpd.conf`), para posibilitar una inmediato funcionamiento con las configuraciones propias.

La opción `-U` (Update) es algo más que una equivalencia a la secuencia `-e-i` (Desinstalar/Eliminar – Instalar). Siempre que sea posible, es preferible usar la opción `-U`.

Atención

Después de cada actualización es necesario controlar las copias de seguridad con las extensiones `.rpmorig` o `.rpmsave` generados por `rpm`. En caso de necesidad transfiera sus ajustes a los nuevos archivos de configuración y elimine después los antiguos con las extensiones `.rpmorig` o `.rpmsave`.

Atención

Para eliminar un paquete se procede de la siguiente manera:

```
rpm -e <paquete>
```

`rpm` sólo borra un paquete en caso de no existir ninguna dependencia. Por lo tanto no es posible suprimir p. ej. `Tcl/Tk` si todavía existe algún programa que lo necesite para su ejecución; esta funcionalidad se debe al “control” por parte de la base de datos RPM.

Si en algún caso excepcional no es posible eliminar un paquete aunque haya dejado de existir toda dependencia, es probable que el problema se resuelva al generar de nuevo la base de datos RPM, usando la opción `--rebuilddb` (las explicaciones sobre la base de datos se pueden ver en el apartado 2 en la página 61).

RPM y parches

Para garantizar la seguridad en la operación de un sistema es necesario instalar periódicamente en el sistema paquetes que lo actualicen. Hasta ahora, un fallo en un paquete sólo podía ser resuelto sustituyendo el paquete entero. En el caso de paquetes grandes con fallos pequeños, podemos encontrarnos rápidamente ante una gran cantidad de datos. A partir de la versión 8.1, SuSE ha incorporado una nueva función a RPM que permiten instalar parches en paquetes.

La información más interesante sobre un parche RPM se mostrará tomando como ejemplo al programa `pine`:

- ¿Es el parche RPM el adecuado para mi sistema?

Para comprobarlo, debe averiguarse en primer lugar la versión instalada del paquete. En el caso de pine, esto sucede con el comando

```
# rpm -q pine
pine-4.44-188
```

A continuación se examina el parche RPM para comprobar si resulta 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
```

Este parche sirve para tres versiones distintas de pine, incluyendo la versión instalada en nuestro ejemplo. Por tanto, el parche puede ser instalado.

- ¿Qué archivos va a sustituir el parche?

Los archivos afectados por el parche pueden leerse fácilmente del parche RPM. El parámetro `-P` de `rpm` sirve para seleccionar características especiales del parche. Así, es posible obtener una lista de los archivos con

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

o, si el parche ya está instalado, con

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

- ¿Cómo se instala un parche RPM en el sistema?

Los parches RPMs se utilizan como RPMs normales. La única diferencia radica en que en el caso de los parches, el RPM apropiado ya debe estar instalado.

- ¿Qué parches están ya instalados en el sistema y a qué versiones de paquetes se han aplicado?

Puede obtener una lista con los parches instalados en el sistema con el comando `rpm -qPa`. Si en un sistema nuevo se ha instalado sólo un parche, como en nuestro ejemplo, la salida del comando será semejante a:

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

Si transcurrido un cierto tiempo quiere saber qué versión del paquete fue instalada en primer lugar, puede consultar la base de datos RPM. En el caso de `pine`, esta información se obtiene con el comando:

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

Puede obtener más información sobre RPM (incluyendo la característica de los parches) en página del manual de `rpm` (`man 1 rpm`) o bien en página del manual de `rpmbuild` (`man 1 rpmbuild`).

Realizar consultas

La opción `-q` (ingl. *query*) permite enviar consultas a los archivos RPM (opción `-p` *<archivo_paquete>*), así como a la base de datos RPM. El tipo de información a consultar depende de las opciones que figuren en la tabla 2.1.

<code>-i</code>	Mostrar información sobre un paquete
<code>-l</code>	Mostrar lista de archivos del paquete
<code>-f</code> <i><Archivo></i>	Consultar por el paquete que contiene el archivo <i><Archivo></i> ; se requiere la especificación de <i><Archivo></i> con su rama completa!
<code>-s</code>	Mostrar estado de los archivos (implica <code>-l</code>)
<code>-d</code>	Nombrar archivos de documentación (implica <code>-l</code>)
<code>-c</code>	Nombrar archivos de configuración (implica <code>-l</code>)
<code>--dump</code>	Mostrar toda la información de verificación de todos los archivos (¡Úselo con <code>-l</code> , <code>-c</code> o <code>-d</code> !)
<code>--provides</code>	Mostrar posibilidades del paquete; otro paquete puede pedir las con <code>--requires</code>
<code>--requires</code> , <code>-R</code>	Mostrar dependencias entre los paquetes
<code>--scripts</code>	Mostrar los distintos scripts de desinstalación

Cuadro 2.1: Las opciones de consulta más importantes (`-q` [`-p`]

...*<paquete>*)

Por ejemplo el comando:

```
rpm -q -i wget
```

da como resultado la salida en pantalla 3:

```
Name       : wget                                elocations: (not relocateable)
Version    : 1.8.1                               Vendor: SuSE AG, Nuernberg, Germany
Release    : 142                                Build Date: Fri Apr  5 16:08:13 2002
Install date: Mon Apr  8 13:54:08 2002 Build Host: knox.suse.de
Group      : Productivity/Networking/Web/Utilities Source RPM:
wget-1.8.1-142.src.rpm
Size       : 2166418                             License: GPL
Packager   : feedback@suse.de
Summary    : A tool for mirroring FTP and HTTP servers
Description:
wget enables you to retrieve WWW documents or FTP files from a server.
This might be done in script files or via command line.
[...]
```

Mensaje en pantalla 3: rpm -q -i wget

La opción `-f` sólo funciona cuando se indica el nombre de archivo completo con la ruta incluida; se pueden indicar tantos archivos como se desee. Por ejemplo el comando:

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

da como resultado:

```
rpm-3.0.3-3
wget-1.5.3-55
```

Si sólo se conoce una parte del nombre del archivo, se puede obtener ayuda mediante un script (ver el archivo 1) al cual se pasa, como parámetro, el nombre del archivo buscado.

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


Fichero 1: Script de búsqueda de paquetes

Con el comando:

```
rpm -q --changelog rpm
```

se puede ver información detallada (actualizaciones, configuración, cambios, etc.) sobre determinados paquetes; en este ejemplo sobre el paquete *rpm*. Sólo se muestran las últimas 5 entradas de la base de datos RPM, el paquete en sí contiene todas las entradas (de los últimos 2 años) – la siguiente consulta funciona si el CD 1 está montado en */cdrom*:

```
rpm -qp --changelog /cdrom/suse/i586/rpm-3*.rpm
```

La base de datos instalada también permite efectuar verificaciones. Éstas se introducen con la opción *-V* (equivalente a *-y o --verify*). Con la verificación, *rpm* muestra todos los archivos del paquete que han sido modificados desde su instalación original. *rpm* coloca hasta ocho caracteres por delante del nombre de archivo que indican los siguientes cambios:

- 5 Número de control MD5
- S Tamaño de archivo
- L Enlace simbólico
- T Tiempo de modificación
- D Número de dispositivo "major" y "minor" (ingl. *device number*)
- U Usuario (ingl. *user*)
- G Grupo (ingl. *group*)
- M Modo (con derecho y tipo)

Cuadro 2.2: Las verificaciones

Para los archivos de configuración aparece como valor adicional la letra *c*, como lo muestra el ejemplo para el archivo */etc/wgetrc* del paquete *wget*, que ha sido modificado:

```
rpm -V wget
```

```
S.5....T c /etc/wgetrc
```

Los archivos de la base de datos RPM se encuentran en */var/lib/rpm*. Estos pueden ocupar hasta 30 MB para una partición */usr* de 1 GB, especialmente

después de una actualización completa. Si la base de datos parece demasiado grande, se puede reducir su tamaño usando la opción `--rebuilddb`. Antes de reconstruir la base de datos se debe hacer una copia de seguridad de la existente.

El script `cron.daily` genera diariamente copias comprimidas de la base de datos y las guarda en `/var/adm/backup/rpmdb`. El número de estas copias está definido por la variable `(MAX_RPMD_DB_BACKUPS)`, cuyo valor por defecto es 5, pero se puede modificar en `/etc/sysconfig/backup`. Cada backup ocupa aproximadamente 3 MB para una partición `/usr` de 1 GB. Se trata de un gasto de espacio que se debe tener en cuenta al determinar el tamaño de la partición raíz, salvo que se cree una partición propia para `/var`.

Instalar y compilar los paquetes fuente

Todos los paquetes con fuentes (ingl. *sources*) de SuSE Linux tienen la extensión `.src.rpm`; estos archivos se llaman "Source-RPMs".

Truco

Los paquetes con fuentes se pueden instalar con YAST como cualquier otro paquete, con la diferencia que estos no se marcan como instalados, con una `[i]`, como ocurre con los paquetes "regulares". Por esta razón los paquetes fuente no figuran en la base de datos RPM, ya que este sólo anota el software *instalado*.

Truco

Si no hay ninguna configuración personal activada (p.ej. a través del archivo `/etc/rpmrc`), los directorios de trabajo de `rpm` o `rpmbuild` deben existir en `/usr/src/packages`. Dichos directorios son:

SOURCES para las fuentes originales (archivos-`.tar.gz`, etc.) y para las adaptaciones específicas de las distintas distribuciones (archivos-`.diff`).

SPECS para los archivos-`.spec`, que controlan el proceso "build" y de este modo actúan como "Makefiles".

BUILD por debajo de este directorio se desempacan o se compilan las fuentes; también se añaden a este los parches.

RPMS en este se graban los paquetes completos en formato binario.

SRPMS y en este los "Source"-RPMs (fuentes).

Al instalar con YqST un paquete de fuentes, todos los componentes necesarios para el proceso “build” se copian en el directorio `/usr/src/packages`: Las fuentes y los parches se van al directorio `SOURCES` y el archivo `.spec` correspondiente se copia en el directorio `SPECS`.

Atención

No haga experimentos con RPM y componentes importantes del sistema como pueden ser paquete `glibc`, paquete `rpm`, paquete `sysvinit` etc.: la operatividad de su sistema está en juego. Para construir paquetes “limpiamente”, utilice paquete `build`. `build` puede crear un entorno de desarrollo separado en el que puede se cambiar con `chroot` y donde puede construir los paquetes deseados sin influir para nada en el sistema activo.

Atención

Tomando como ejemplo el paquete `wget.src.rpm`, después de ser instalado con YqST, aparecerán los siguientes archivos:

```
/usr/src/packages/SPECS/wget.spec
/usr/src/packages/SOURCES/wget-1.4.5.dif
/usr/src/packages/SOURCES/wget-1.4.5.tar.gz
```

Con el comando `rpmbuild -b <X> /usr/src/packages/SPECS/wget.spec` comienza la compilación. La variable `<X>` puede representar diferentes pasos, de los cuales aquí figuran algunos (ver también la ayuda que aparece con la opción `-help` o la documentación de RPM):

- bp prepara las fuentes en el directorio `/usr/src/packages/BUILD`; las desempaqueta y pone los parches
- bc igual a -bp, pero con compilación.
- bi igual a -bc, pero con instalación del paquete. ¡Cuidado: Si hay algún paquete que no soporte la característica *BuildRoot*, es posible que durante la instalación se sobrescriban algunos archivos de configuración importantes!
- bb igual a -bi, pero con generación adicional del “Binary-RPM” que, en caso de éxito, se encuentra en el directorio `/usr/src/packages/RPMS`.
- ba igual a -bb, pero genera adicionalmente el “Source-RPM” que se encuentra, en caso de éxito, en el directorio `/usr/src/packages/SRPMS`.

La opción `--short-circuit` permite saltarse determinados pasos.

El “Binary-RPM” se instala finalmente con `rpm -i`, o mejor con `rpm -U`.

Creación de paquetes RPM con build

Al construir muchos paquetes se corre el riesgo de que se instalen archivos no deseados en el sistema. Para evitarlo se puede emplear el paquete `paquete build`, el cual crea un entorno definido dentro del que se contruye el paquete. Para crear este entorno "chroot", se debe proporcionar un árbol completo de paquetes al script `build`, ya sea en el disco duro, mediante NFS o desde un DVD. La ubicación concreta se comunica al script por medio del comando `build --rpms <ruta>`. A diferencia de `rpm`, el comando `build` quiere tener el archivo SPEC en el mismo directorio que las fuentes. Para volver a compilar `wget` en el ejemplo superior con el DVD montado en el sistema en `/media/dvd`, ejecute los siguientes comandos como usuario `root`:

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

A continuación se creará en `/var/tmp/build-root` un entorno mínimo donde se construirá el paquete. Los paquetes resultantes se almacenarán posteriormente en `/var/tmp/build-root/usr/src/packages/RPMS`

El script `build` ofrece además otras opciones. Así, se puede definir la utilización de los propios RPMs frente al resto, omitir la iniciación del entorno `build` o restringir el comando `rpm` a una de las fases descritas anteriormente. Puede obtener más información con el comando `build --help` y en página del manual de `build` (`man 1 build`).

Herramientas para los archivos RPM y la base de datos RPM

El Midnight Commander (`mc`) puede mostrar el contenido de un archivo RPM y copiar partes de él. El archivo RPM se muestra en un sistema de archivos virtual para el cual se ponen a disposición todas las opciones del menú del `mc`. La información de los encabezamientos del "archivo" `HEADER` se visualiza con (F3); con las teclas del cursor y (J) se puede "navegar" por la estructura del archivo y en caso de necesidad, copiar componentes usando (F5). – Por otra parte, ya existe `rpm.el` para Emacs, que es un "frontal" para `rpm`

KDE incluye la herramienta `kpackage`. En GNOME se incluye `gnorpm`.

`Alien` (`alien`) permite la conversión de los formatos de las distintas distribuciones. Con este programa se puede intentar convertir, *antes* de la instalación, los archivos antiguos del tipo TGZ al formato RPM, para que la base de datos RPM reciba *durante* la instalación la información de los paquetes. Pero cuidado: `alien` es un script de Perl y según sus autores todavía se encuentra en fase alfa, aunque ya ha alcanzado un número de versión bastante alto.

Parte II

Configuración

YaST en modo texto (ncurses)

Este capítulo está dirigido a administradores de sistemas y expertos que no disponen de un servidor X en su ordenador y por tanto deben utilizar la herramienta de instalación en modo texto.

En este capítulo se incluye información básica para trabajar con YaST en modo texto (ncurses). Además le explicaremos cómo se puede actualizar su sistema online de forma automática.

Funcionamiento	68
Trabajar con los módulos	69
Arranque de módulos individuales	70
La actualización online de YaST	71

Funcionamiento

El funcionamiento puede resultar algo raro al principio pero es de hecho muy sencillo. Con las teclas **(Tab)**, **(Alt) + (Tab)**, **(Espacio)**, flechas de dirección (**(↑)** o **(↓)**) y **(Intro)**, así como con los atajos de teclado, se puede manejar en principio todo el programa. Si arranca YaST en modo texto, lo primero que aparece es la ventana principal (véase figura 3.1).

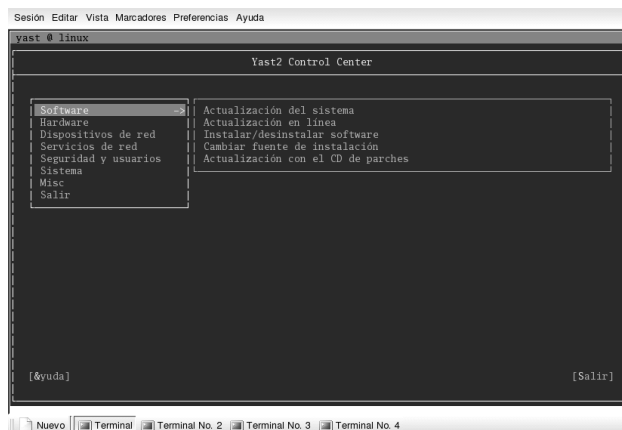


Figura 3.1: La ventana principal de YaST-ncurses

Aquí pueden observar tres áreas: En la parte izquierda, enmarcada por una gruesa línea blanca, se presentan las categorías en las que están clasificados los distintos módulos. La categoría activa está resaltada por un fondo de color. A la derecha, enmarcados por un fino cuadro blanco, se encuentran los módulos correspondientes a la categoría activa. En la parte inferior están los botones de ‘Ayuda’ y ‘Salir’.

Después de iniciar por primera vez el Centro de Control de YaST, se selecciona automáticamente la categoría de ‘Software’. Puede cambiar de categoría con las teclas **(↓)** y **(↑)**. Para iniciar un módulo de la categoría seleccionada pulse la tecla **(→)**. La lista de módulos aparece ahora enmarcada con una línea gruesa. Seleccione el módulo deseado con las teclas **(↓)** y **(↑)**. El pulsar de manera continua las teclas de flechas le permite “navegar” por la lista de módulos disponibles. Una vez que un módulo ha sido seleccionado, su nombre aparece resaltado en color y en la ventana inferior aparece una breve descripción del mismo.

Con la tecla **(Intro)** puede iniciar el módulo deseado. Los diversos botones o campos de selección del módulo contienen una letra de otro color (amarillo en la

configuración por defecto). La combinación **(Alt) + (letra_amarilla)** le permite seleccionar directamente el botón en cuestión sin tener que navegar con **(Tab)**.

Abandone el Centro de Control de YaST con el botón 'Salir' o seleccionando el punto 'Salir' en la lista de categorías y pulsando a continuación **(Intro)**.

Limitaciones de las combinaciones de teclas

Si en su sistema con un servidor X en funcionamiento se puede utilizar combinaciones de teclas con ALT, puede que estas no funcionen con YaST. Además puede que teclas como **(Alt)** o **(↑)** ya estén ocupadas por otras configuraciones del terminal que se utiliza.

(Alt) en lugar de (Esc): Las combinaciones con Alt pueden realizarse con **(Esc)** en vez de **(Alt)**, p. ej. **(Esc) + (h)** en vez de **(Alt) + (h)**.

Saltar hacia adelante o hacia atrás con (Control) + (f) y (Control) + (b): En caso de que las combinaciones con **(Alt)** y **(↑)** ya estén ocupadas por el gestor de ventanas o el terminal, utilice de forma alternativa las combinaciones **(Control) + (f)** (hacia adelante) y **(Control) + (b)** (hacia atrás).

Limitaciones de las teclas de función: En SuSE Linux 9.0 las teclas F también están ocupadas con funciones (véase abajo). También aquí puede que determinadas teclas F ya estén ocupadas según el terminal escogido y por lo tanto no estén disponibles para YaST. Sin embargo en una consola de texto, las combinaciones con **(Alt)** y las teclas de función deberían estar totalmente disponibles.

A continuación, se parte de que las combinaciones de teclas con **(Alt)** funcionan correctamente.

Trabajar con los módulos

Navegación entre botones/listas de selección: Con **(Tab)** y **(Alt) + (Tab)** puede navegar entre los botones y los cuadros de listas de selección.

Navegación por listas de selección: Siempre que esté en un cuadro activo en el que se encuentre una lista de selección, se puede mover con las teclas de dirección **(↑)** y **(↓)** entre los distintos elementos, p. ej. entre los módulos de un grupo de módulos en el centro de control.

Activar botones y casillas de control La selección de botones con un corchete vacío (casillas de control) o de aquellos con un paréntesis redondo se realiza con **(Espacio)** o **(Intro)**. La selección de botones en la parte inferior de los módulos se realiza con **(Intro)** cuando están seleccionados (en color verde), o más rápidamente, con la combinación **(Alt) + (letra_amarilla)** (véase la Figura 3.2).

Las teclas de función: Las teclas F (de **(F1)** a **(F12)**) están asimismo ocupadas con funciones. Sirven de acceso rápido a los distintos botones disponibles. Qué teclas F están ocupadas con qué funciones depende del módulo de YaST en el que se encuentre, ya que se ofrecen distintos botones en cada módulo (p. ej. detalles, infos, añadir, eliminar...). La Ayuda de YaST, a la que puede acceder con **(F1)**, le proporciona información sobre las funciones que hay en cada tecla F.

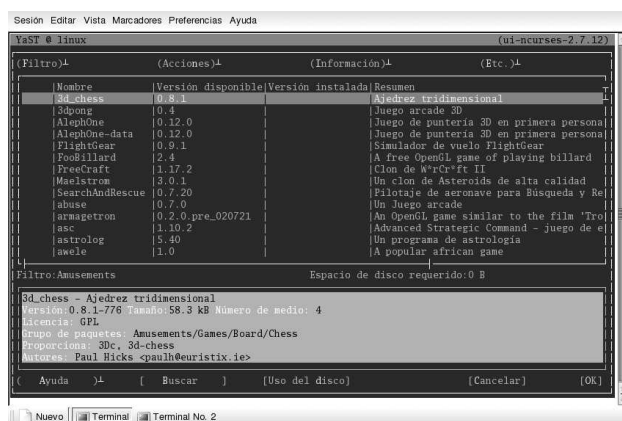


Figura 3.2: El módulo de instalación de software

Arranque de módulos individuales

Para ahorrar tiempo, los módulos de YaST se pueden iniciar individualmente. Basta con introducir:

```
yast <nombremódulo>
```

El módulo de red p. ej. se arranca con `yast lan`.

Puede obtener una lista con el nombre de todos los módulos disponibles en su sistema con `yast -l` o con `yast --list`.

La actualización online de YaST

La actualización en línea de YaST (YOU – YaST Online Update) puede controlarse e iniciarse desde una consola. Como usuario `root`, puede utilizar el comando

```
tierra:/root # yast2 online_update .auto.get
```

para recibir desde el servidor que se encuentre en primera posición en la lista `/etc/suseservers` la lista de los parches actuales de todos los rpm. Si sólo quiere cargar unos determinados parches, se pueden utilizar opciones adicionales como `security`, `recommended`, `document`, `YaST` y `optional`. `security` sólo carga parches relacionados con la seguridad; `recommended` sirve para cargar los parches que SuSE recomienda; `document` ofrece información sobre los parches o el servidor FTP; `YaST` sólo carga los parches para YaST; y con `optional` se cargan los parches de menor importancia.

La información sobre los parches se guarda en `/var/lib/YaST2/you/<arch>/update/<versión>/patches`. Sólo `root` está autorizado a leerlos; `<versión>` representa la versión de SuSE Linux en cuestión. `<arch>` se refiere a la arquitectura del ordenador en el que utiliza SuSE Linux.

El comando para descargar p. ej. los parches de seguridad es:

```
tierra:/root # yast2 online_update .auto.get security
```

Cada vez que utiliza `.auto.get`, se actualiza la lista de los servidores FTP en `/etc/suseservers`. Para desactivarlo, modifique dentro del fichero `/etc/sysconfig/onlineupdate` la línea:

```
tierra:/root # YAST2_LOADFTPSERVER="yes"
```

poniendo `no` en lugar de `yes`.

La instalación de los parches se lleva a cabo mediante:

```
tierra:/root # yast2 online_update .auto.install
```

Con este comando se instalan todos los parches que se hayan bajado de Internet. Para instalar un sólo un determinado grupo de parches, se pueden utilizar las mismas opciones como en el caso de `.auto.get`.

La ventaja de este método es la automatización; como administrador de sistema tiene la posibilidad de descargar los paquetes p. ej. durante la noche e instalarlos a la mañana siguiente.

Cronjobs para YOU

Puesto que no todo el que quiere o debe utilizar YOU está familiarizado con cronjobs, a continuación presentamos una breve introducción. Existen principalmente dos posibilidades para un cronjob; aquí se describe la más sencilla:

1. Entre al sistema como `root`
2. Arranque el editor de Crontab con el comando `crontab -e`.
3. Escriba `i` para acceder al modo de inserción del programa `vi`
4. Introduzca las siguientes líneas:

```
MAILTO="" "  
13 3 * * 0 /sbin/yast2 online_update auto.get  
53 3 * * 0 /sbin/yast2 online_update auto.install
```

Las primeras 5 posiciones de las dos últimas líneas indican de izquierda a derecha: 13=minutos, 3=horas, *=es igual el día del mes, *=es igual el mes del año, 0=domingo. Esto quiere decir que se iniciará un Cronjob cada domingo a las 3 horas y 13 minutos de la noche. Por tanto la siguiente entrada indica 40 minutos después, los domingos a las 3 horas y 53 minutos. La línea `MAILTO="" "` impide que `root` reciba un mail de YaST-ncurses, por lo que puede quedar vacío.

Aviso

Introduzca la hora para los Cronjobs arbitrariamente, es decir, no es necesario que sea la misma hora que en el ejemplo anterior, ya que de ser así habría una sobrecarga en el servidor FTP, o se rebasaría el número máximo de accesos que se pueden realizar simultáneamente.

Aviso

5. Guarde el Cronjob con la siguiente sucesión de teclas (una detrás de otra) `(Esc) :wq` seguido de `(↵)` o bien `(Esc) ZZ`.

El daemon Cron se reiniciará automáticamente y su Cronjob quedará guardado en el fichero `/var/spool/cron/tabs/root`.

El proceso de arranque y el gestor de arranque

En este capítulo se presentan diferentes métodos para arrancar el sistema. Para que se pueda comprender cada uno de ellos, al principio se explican algunos detalles sobre el proceso de arranque. Después pasa a describirse detalladamente el gestor de arranque actual GRUB y su predecesor LILO.

El proceso de arranque en el PC	74
Concepto de arranque	75
Archivos map, GRUB y LILO	76
El arranque con GRUB	77
Arrancar con LILO	87
Configuración de LILO	88
Crear un CD de arranque	95

El proceso de arranque en el PC

Después de encender el ordenador, la BIOS ((ingl. *Basic Input Output System*)) inicia la pantalla y el teclado y comprueba la memoria RAM. Hasta este momento el ordenador aún no utiliza ningún medio de almacenamiento (disquete, disco duro).

A continuación, de los valores que están en la CMOS (*CMOS setup*) se lee la información sobre los periféricos más importantes, la hora y la fecha. En este momento se ha de conocer ya el primer disco duro y su geometría, así que la carga del sistema operativo desde este disco puede comenzar.

Para ello se lee desde el primer disco duro, el primer sector físico de datos del tamaño de 512 bytes y se carga a la memoria. El control pasa a este pequeño programa y la ejecución de los comandos en este determina a partir de ahora el proceso de arranque. Estos primeros 512 bytes en el primer disco duro se denominan en inglés *Master Boot Record* (MBR).

Hasta el mismo momento de cargar el MBR, el arranque es exactamente el mismo en cualquier PC y completamente independiente del sistema operativo instalado; el ordenador sólo tiene acceso a los dispositivos a través de las rutinas (drivers) grabadas en la BIOS.

Master Boot Record

La estructura del MBR está definida por una convención independiente de los sistemas operativos. Los primeros 446 bytes están reservados para código de programas. Los próximos 64 bytes ofrecen espacio para una tabla de particiones con hasta 4 entradas; apartado [Particionar para usuarios avanzados](#) en la página 26. Sin la tabla de particiones no puede existir ningún sistema de archivos, es decir, es prácticamente imposible usar el disco duro. Los últimos 2 bytes deben contener una "cifra mágica" (AA55): un MBR que tenga otra cifra será tratado como no válido por parte de la BIOS y de todos los sistemas operativos de PC

Sectores de arranque

Los sectores de arranque son los primeros de cada partición, a excepción de la partición extendida que es un "contenedor" para otras particiones. Los sectores de arranque ofrecen 512 bytes de espacio y sirven para albergar código, que puede ser ejecutado por el sistema operativo que resida en esta partición. En el caso de los sectores de arranque de DOS, Windows u OS/2, esto es realmente así y aparte del código ejecutable también contienen información importante del

sistema de archivos. Por el contrario, los sectores de arranque de una partición Linux están en principio vacíos (!), incluso después de haber generado el sistema de archivos. Por lo tanto, una partición Linux *no es autoarrancable* aunque tenga un kernel y un sistema de archivos raíz válidos.

Un sector de arranque con código de arranque válido lleva en los últimos 2 bytes la misma "cifra mágica" que el MBR (AA55).

Arranque de DOS o Windows 95/98

En el MBR de DOS del primer disco duro hay una entrada de partición marcada como *activa* (ingl. *bootable*), es decir, que se busca allí el sistema a cargar por lo que DOS debe estar instalado, en todo caso, en el primer disco duro. El código de programa de DOS en el MBR representa el primer paso del Bootloader (ingl. *first stage bootloader*) y comprueba si se encuentra un sector de arranque válido en la partición indicada.

Si fuera el caso, el código en este sector de arranque se ejecuta como segundo paso del Bootloader (ingl. *secondary stage loader*). Este código carga los programas de sistema y finalmente aparece el conocido prompt del DOS o la interfaz gráfica de Windows 95/98.

En DOS una sola partición primaria puede ser marcada como activa, lo cual significa que el sistema DOS no puede residir en una unidad lógica dentro de una partición extendida.

Concepto de arranque

El "concepto de arranque" más simple que uno se puede imaginar es el de un ordenador con un solo sistema operativo. Para este caso, acabamos de comentar los procesos que transcurren durante el inicio. Un proceso de arranque semejante también sería imaginable para un ordenador de "sólo-Linux" y en este caso no sería necesaria la instalación de GRUB o LILO. Pero no se podría indicar al kernel una línea de comandos para el inicio (con información adicional sobre el hardware o con indicaciones especiales respecto al arranque, etc.).

En cuanto existen varios sistemas operativos instalados en un ordenador, existen también diferentes conceptos de arranque:

Arrancar sistemas operativos adicionales de disquete El primer sistema operativo se carga desde el disco duro y los demás desde la disquetera usando un disquete de arranque.

- *Condición:* Existe una disquetera desde la cual se puede arrancar.
- *Ejemplo:* Linux se instala como sistema adicional a Windows y se arranca siempre desde un disquete de arranque.
- *Ventajas:* Se ahorra la instalación del gestor de arranque.
- *Desventajas:* Se debe mantener *siempre* un buen stock de disquetes de arranque que funcionen y el arranque tarda más.
- El hecho de que Linux no pueda arrancar sin el disquete de arranque puede ser una ventaja tanto como una desventaja según las condiciones de uso.
- Arrancar sistemas adicionales de un medio de almacenamiento USB. La información necesaria para arrancar puede leerse de un medio de almacenamiento USB de la misma forma que desde un disquete.

Instalación de un gestor de arranque Un gestor de arranque (ingl. *bootmanager*), permite mantener varios sistemas operativos en un ordenador y alternar entre ellos. El usuario selecciona el sistema operativo durante el arranque; para cambiar de sistema operativo se debe reiniciar el ordenador. La condición previa es que el gestor de arranque que se elija se "adapte" a todos los sistemas operativos instalados.

Archivos map, GRUB y LILO

El mayor problema al arrancar el sistema operativo consiste en que el kernel se encuentra en un archivo dentro de un sistema de archivos dentro de una partición dentro de un disco duro. Sin embargo, para la BIOS los conceptos de sistema de archivos y particiones son totalmente desconocidos.

Para solucionar este problema, se crearon los denominados "maps" y "archivos map". En los mapas se anotan los bloques físicos del disco duro que contienen los archivos lógicos. Cuando se trabaja con uno de estos mapas, la BIOS carga los bloques físicos en el mismo orden en que se encuentran en el archivo de mapas, y de este modo produce los archivos lógicos en la memoria.

La diferencia fundamental entre LILO y GRUB consiste en que LILO confía casi por completo en los mapas, mientras que GRUB intenta liberarse de los mapas fijos durante el arranque lo más rápidamente posible. GRUB consigue hacer esto mediante el *código del sistema de archivos* (ingl. *file system code*), que le posibilita acceder a los archivos a través de la ruta y no mediante los números de bloque.

Esta diferencia tiene un fundamento histórico. En los primeros días de Linux existían muchos sistemas de archivos distintos que se peleaban por la supremacía.

Werner Almesberger desarrolló un gestor de arranque (LILO) que no necesitaba saber el tipo de archivos en que se encontraba el kernel que se quería arrancar. La idea que se esconde detrás de GRUB se remonta más atrás, a los días del Unix y BSD tradicionales. Estos sistemas se habían acostumbrado a un determinado tipo de sistema de archivos y, desde el principio, habían reservado un espacio para el gestor de arranque. Este gestor conocía la estructura del sistema de archivos al que estaba ligado, por lo que era capaz de encontrar el kernel con su nombre en el directorio root.

En el siguiente apartado se describe la instalación y configuración de un gestor de arranque tomando como ejemplo al gestor GRUB. A continuación se describirán las diferencias con respecto al uso de LILO. Una descripción más detallada de LILO se encuentra en ?. Las indicaciones se encuentran en: `/usr/share/doc/packages/lilo/user.dvi`. Puede leer el texto en la pantalla con programas como `kdivi` o imprimirlo con el comando `lpr /usr/share/doc/packages/lilo/user.dvi`.

Atención

¿Cuándo hay que instalar qué cargador de arranque?

En caso de que actualice desde una versión anterior de SuSE Linux en la que se utilizaba LILO, se recomienda volver a instalar LILO. En el caso de una nueva instalación se emplea GRUB, a no ser que la partición raíz se instale en los siguientes sistemas Raid:

- Controladora Raid dependiente del CPU (como por ejemplo numerosas controladoras Promise o Highpoint)
- Software Raid
- LVM

Atención

El arranque con GRUB

Al igual que LILO, GRUB (ingl. *Grand Unified Bootloader*) está compuesto por dos etapas: la primera ("stage1") es de 512 bytes y está guardada en el MBR o en el bloque de arranque de una partición de disco o disquete; la segunda etapa ("stage2"), más grande, se carga a continuación y contiene el código del programa. En GRUB, la única función de la primera etapa es cargar la segunda etapa del cargador de arranque.

Pero a partir de este punto, GRUB se diferencia de LILO, ya que stage2 puede acceder directamente al sistema de archivos. Actualmente, se soportan ext2, ext3, reiser FS, jfs, xfs, minix y el sistema DOS FAT FS utilizado por Windows. GRUB puede acceder a los sistemas de archivos en los dispositivos de disco BIOS soportados (disquetes o discos duros detectados por la BIOS) antes de arrancar, por lo que los cambios en el archivo de configuración de GRUB no obligan a reinstalar el gestor de arranque. Al arrancar, GRUB vuelve a cargar los archivos de menú incluyendo las rutas y particiones actuales hacia el kernel o el ramdisk de inicio (`initrd`) y encuentra estos archivos automáticamente.

GRUB presenta la enorme ventaja de que es posible cambiar todos los parámetros de arranque *antes* de arrancar. Por ejemplo, si se ha cometido un error al editar el archivo de menús, puede resolverse fácilmente de este modo. Además se permite introducir los comandos de arranque de forma interactiva mediante una especie de cursor. De esta forma puede arrancar sistemas operativos que todavía no dispongan de una entrada propia en el menú de arranque. GRUB le ofrece la posibilidad de comprobar el estado del kernel e `initrd` antes de arrancar.

El menú de arranque de GRUB

Tras la pantalla de bienvenida con el menú de arranque se encuentra el archivo de configuración de GRUB, `/boot/grub/menu.lst`. Este archivo contiene toda la información sobre otras particiones o sistemas operativos que pueden ser arrancados con ayuda del menú.

En cada arranque del sistema, GRUB vuelve a leer el archivo de menú del sistema de archivos. Por lo tanto, no hay ninguna necesidad de actualizar GRUB después de modificar el archivo; sencillamente utilice YaST2 o su editor favorito para realizar los cambios.

Este archivo de menú contiene comandos de sintaxis es muy sencilla. Cada línea incluye un comando seguido de los parámetros opcionales separados por espacios en blanco, al igual que en la shell. Por razones históricas, algunos comandos tienen un signo de igualdad como primer parámetro. Las líneas de comentarios comienzan con `'#'`.

Para reconocer las entradas de menú en la vista del menú, debe dar un nombre o `title` a cada entrada. El texto que aparece tras la palabra clave `title` será mostrado (incluyendo espacios en blanco) en el menú como opción para seleccionar. Después de seleccionar una entrada determinada del menú, se ejecutarán todos los comandos que se encuentren antes del siguiente `title`.

El caso más sencillo es la ramificación al cargador de arranque de otro sistema operativo. El comando es `chainloader` y el argumento suele ser el bloque de

arranque de otra partición en GRUBs *anotación por bloque* (ingl. *block-notation*), por ejemplo:

```
chainloader (hd0,3)+1
```

Los nombre de dispositivo que se encuentran en GRUB se explican en el apartado [Convención de nombres para discos duros y particiones](#) en esta página. El ejemplo anterior determina el primer bloque de la cuarta partición del primer disco duro.

Con el comando `kernel` se puede especificar una copia o imagen del kernel (ingl. *kernel image*). El primer argumento es la ruta a la copia del kernel de una partición. El resto de los argumentos mostrarán el kernel en la línea de comandos.

Si en el kernel no está compilado el controlador adecuado para el acceso a la partición `root`, se debe introducir `initrd`. Aquí se trata de un comando GRUB que tiene la ruta al archivo `initrd` como único argumento. Puesto que la dirección de carga del `initrd` se encuentra en la copia del kernel cargada, el comando `initrd` debe seguir a `kernel`.

El comando `root` facilita la especificación de los archivos del kernel y de `initrd`. `root` tiene como único argumento un dispositivo GRUB o una partición de éste. Todas las rutas del kernel, de `initrd` o de otros archivos en las que no se ha introducido explícitamente un dispositivo, anticiparán el dispositivo hasta el siguiente comando `root`. Este comando no aparece en un `menu.lst` generado durante la instalación.

Al final de cada entrada de menú se encuentra implícito el comando `boot`, por lo que no es necesario escribirlo en el archivo de menú. Si tiene ocasión de utilizar GRUB de forma interactiva en el arranque, debe introducir el comando `boot` al final. `boot` no tiene argumentos, simplemente controla la copia cargada del kernel o el "chain loader" indicado.

Si ha introducido todas las entradas de menú, debe fijar una entrada como `default` o predeterminada. De no ser así, se utilizará la primera (entrada 0) como valor predeterminado. También tiene la posibilidad de asignar un tiempo de espera en segundos (`timeout`) antes de que se inicie el arranque de la opción predeterminada. `timeout` y `default` se escriben normalmente antes de las entradas de menú. Puede encontrar un ejemplo explicado de un archivo en la sección [Ejemplo de un archivo de menú](#) en la página 81.

Convención de nombres para discos duros y particiones

Para denominar a los discos duros y particiones, GRUB utiliza convenciones distintas a las ya habituales de los dispositivos Linux "normales" (por ejemplo

/dev/hda1). El primer disco duro se denomina siempre `hd0`, la unidad de disquetes `fd0`.

Atención

Numeración de las particiones en GRUB

La numeración de las particiones en GRUB empieza por cero. (`hd0, 0`) corresponde a la primera partición en el primer disco duro. En una estación de trabajo ordinaria a la que esté conectado un disco como "Primary Master", el nombre de dispositivo es `/dev/hda1`.

Atención

Las cuatro particiones primarias posibles ocupan los números de particiones 0 a 3. Las particiones lógicas se designan con los números a partir de 4:

(<code>hd0,0</code>)	primera partición primaria en el primer disco duro
(<code>hd0,1</code>)	segunda partición primaria
(<code>hd0,2</code>)	tercera partición primaria
(<code>hd0,3</code>)	cuarta partición primaria (y normalmente partición extendida)
(<code>hd0,4</code>)	primera partición lógica
(<code>hd0,5</code>)	segunda partición lógica
...	

Atención

IDE, SCSI o RAID

GRUB no distingue entre dispositivos IDE, SCSI o RAID. Todos los discos duros detectados por la BIOS u otras controladoras se numeran según el orden de arranque definido en la BIOS.

Atención

El problema, tanto en LILO como en GRUB, es que no resulta fácil realizar la correspondencia entre los nombres de dispositivos Linux y los nombres de dispositivo de la BIOS. Ambos utilizan algoritmos parecidos para generar esta asignación. No obstante, GRUB guarda esta correspondencia en un archivo (`device.map`) que puede ser editado. Para encontrar más información sobre `device.map`, consulte la sección [El archivo `device.map`](#) en la página 83.

Una ruta completa de GRUB consta de un nombre de dispositivo que se escribe entre paréntesis así como de la ruta del archivo del sistema de archivos a la partición indicada. Al principio de la ruta se coloca una barra. Por ejemplo, en un sistema con un solo disco duro IDE y Linux en la primera partición, el kernel arrancable será:

```
(hd0,0)/boot/vmlinuz
```

Ejemplo de un archivo de menú

Para comprender mejor la estructura de un archivo de menú GRUB, presentamos a continuación un breve ejemplo. El sistema de nuestro ejemplo contiene una partición de arranque de Linux en `/dev/hda5`, una partición root en `/dev/hda7` y un sistema 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 se ocupa de la configuración de la pantalla de bienvenida:

gfxmenu (hd0,4)/message La imagen de fondo se encuentra en `/dev/hda5` y se llama `message`

color white/green black/light-gray El esquema de colores: blanco (primer plano), azul (fondo), negro (selección) y gris claro (fondo de la selección). El esquema de colores no se ve reflejado en la pantalla de bienvenida sino al salir de ella con `(Esc)`.

default 0 Por defecto se arranca la primera entrada del menú con `title linux`.

timeout 8 Si transcurren 8 segundos sin que el usuario realice ninguna acción, GRUB arrancará automáticamente.

El segundo bloque (y también el más grande) contiene una lista con los diversos sistemas operativos arrancables.

- La primera entrada (`title linux`) se encarga del arranque de SuSE Linux. El kernel (`linux`) se encuentra en la primera partición lógica (aquí la partición de arranque) del primer disco duro. Aquí se añaden los parámetros del kernel como la especificación de la partición raíz, el modo VGA, etc. La definición de la partición raíz se realiza de acuerdo con el esquema Linux (`/dev/hda7/`), ya que esta información va dirigida al kernel y no tiene mucha relación con GRUB. `initrd` se encuentra también en la primera partición lógica del primer disco duro.
- La segunda entrada se ocupa de cargar Windows. Este sistema operativo se inicia desde la primera partición del primer disco duro (`hd0, 0`). La carga y ejecución del primer sector de la partición especificada se controla por medio de `chainloader +1`.
- La siguiente sección permite el arranque desde un disquete sin tener que cambiar la configuración de la BIOS.
- La opción de arranque `failsafe` sirve para iniciar Linux con una selección determinada de parámetros del kernel que permiten el arrancar Linux incluso en sistemas problemáticos.

El archivo de menú puede modificarse en cualquier momento; GRUB lo aplicará automáticamente la próxima vez que arranque el sistema. Si desea editar este archivo con carácter permanente, puede utilizar cualquier editor o bien YaST. Si sólo desea efectuar cambios temporales, puede hacerlo de forma interactiva con la función `edit` de GRUB.

Modificar las entradas de menú

Por medio de las teclas de cursor puede seleccionar en el menú gráfico de GRUB el sistema operativo que debe ser arrancado. Si selecciona un sistema Linux, puede añadir sus propios parámetros en el cursor de arranque como en LILO. No obstante, GRUB va incluso más allá de este concepto: pulse (`Esc`) para salir de la pantalla de bienvenida e introduzca a continuación (`e`) (`edit`). Una vez hecho esto podrá editar directamente cada una de las entradas del menú. Ahora bien, los cambios realizados sólo tienen validez para ese proceso de arranque y no se adoptarán de forma permanente.

Atención

Disposición del teclado durante el proceso de arranque

Tenga presente que al arrancar estará trabajando con un teclado norteamericano. Preste atención a los caracteres especiales intercambiados.

Atención

Después de activar el modo de edición, seleccione por medio de las teclas de cursor la entrada del menú cuya configuración desea modificar. Para acceder a la configuración en modo de edición ha de volver a pulsar (e). De este modo, puede corregir datos incorrectos de las particiones o rutas antes de que los fallos repercutan negativamente en el proceso de arranque. Para salir del modo de edición y volver al menú de arranque pulse (Intro). A continuación arranque esa entrada por medio (b). Un texto de ayuda en la parte inferior de la pantalla le informa sobre el resto de opciones de las que dispone.

Si desea guardar de forma permanente las opciones de arranque modificadas, abra el archivo `menu.lst` como usuario `root` y añada los parámetros del kernel adicionales a la línea existente separándolos entre sí con espacios:

```
title linux
    kernel (hd0,0)/vmlinuz root=/dev/hda3 <parámetros adicionales>
    initrd (hd0,0)/initrd
```

La próxima vez que el sistema arranque, GRUB cargará automáticamente los nuevos parámetros. Otra posibilidad para los cambios consiste en activar el módulo del cargador de arranque de YAST. En este procedimiento, el parámetro también es añadido a una línea ya existente separándolo mediante un espacio.

El archivo `device.map`

El ya mencionado archivo `device.map` contiene la correspondencia entre los nombres de dispositivo GRUB y los nombres de dispositivo Linux. Si dispone de un sistema mixto con discos duros IDE y SCSI, GRUB debe intentar averiguar el orden de arranque a partir de un procedimiento concreto. En este caso, GRUB no tiene acceso a la información relevante de la BIOS. GRUB guarda el resultado de esta comprobación en `/boot/grub/device.map`. A continuación vemos un ejemplo para el que asumimos que el orden de arranque definido en la BIOS es de IDE antes que SCSI:

```
(fd0) /dev/fd0
(hd0) /dev/hda
(hd1) /dev/hdb
(hd2) /dev/sda
(hd3) /dev/sdb
```

Si al arrancar el sistema se producen problemas, compruebe el orden de arranque y modifíquelo si es necesario con ayuda de la shell GRUB. Si el sistema Linux arranca en primer lugar, puede modificar el archivo `device.map`

de forma permanente mediante el módulo del cargador de arranque de YQST o cualquier editor.

Tras modificar el archivo `device.map` manualmente, ejecute el siguiente comando para reinstalar GRUB:

```
grub --batch < /etc/grub.conf
```

El archivo `/etc/grub.conf`

`/etc/grub.conf` es el tercer archivo de configuración más importante de GRUB por detrás de `menu.lst` y `device.map`. Este archivo contiene las opciones y los parámetros que `grub` necesita para instalar correctamente el cargador de arranque:

```
root (hd0,4)
install /grub/stage1 d (hd0) /grub/stage2 0x8000 (hd0,4)/grub/menu.lst
quit
```

A continuación se explica el significado de cada una de las entradas:

root (hd0,4) Con este comando se le indica a GRUB que los comandos que vienen a continuación se refieren sólo a la primera partición lógica del primer disco duro donde GRUB encontrará sus archivos de arranque.

install *<parameter>* El comando `grub` ha de iniciarse con el parámetro `install`. `stage1` ha de ser instalado en el MBR del primer disco duro como primera etapa del cargador de arranque (`/grub/stage1 d (hd0)`). `stage2` ha de cargarse en la dirección de memoria `0x8000` (`/grub/stage2 0x8000`). La última entrada (`(hd0,4)/grub/menu.lst`) informa a `grub` de la ubicación del archivo de menú.

La shell GRUB

Existen dos variantes de GRUB: una como cargador de arranque y otra como un programa normal Linux en `/usr/sbin/grub`. Este programa se denomina *shell GRUB*. La funcionalidad de instalar GRUB como cargador de arranque en un disco duro o disquete está directamente integrada en GRUB en forma del comando `install` o `setup`. De este modo, esta función está disponible en la shell GRUB cuando Linux se está ejecutando. No obstante, estos comandos también están disponibles *durante* el proceso de arranque sin necesidad de que Linux se esté ejecutando, lo que simplifica en gran medida la recuperación de un sistema defectuoso.

El algoritmo de correspondencia se activa sólo cuando la shell GRUB se ejecuta como programa Linux. El programa lee el archivo `device.map`, el cual está formado por líneas con los nombres de dispositivo GRUB y Linux respectivos. Puesto que el orden de arranque de IDE, SCSI y otros discos duros depende de muchos factores y Linux no puede reconocer la correspondencia, es posible definir el orden en el archivo `device.map`. Si se producen problemas al arrancar, compruebe si el orden reflejado en este archivo coincide con el orden definido en la BIOS. El archivo se encuentra en el directorio GRUB `/boot/grub/`). Puede obtener información adicional en la sección [El archivo `device.map`](#) en la página 83.

Definir la contraseña de arranque

GRUB soporta el acceso a sistemas de archivos ya desde el mismo momento del arranque. Esto también significa que es posible ver algunos archivos del sistema Linux a los que los usuarios sin privilegios root no tendrían acceso normalmente en un sistema iniciado. Mediante la definición de una contraseña, no sólo puede evitar este tipo de accesos no autorizados durante el proceso de arranque, sino también bloquear la ejecución de determinados sistemas operativos por parte de los usuarios.

Para definir una contraseña de arranque, realice los siguientes pasos como usuario `root`:

- Codifique la contraseña en la shell GRUB:

```
grub> md5crypt
Password: ****
Encrypted: $1$lS2dv/$J0YcdxIn7CJk9xShzzJVw/
```

- Introduzca el valor codificado 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/$J0YcdxIn7CJk9xShzzJVw/
```

De esta forma se impide la ejecución de comandos GRUB en el cursor de arranque. Para poder volver a ejecutar comandos es necesario introducir  y la contraseña. No obstante, aquí sigue siendo posible para todos los usuarios el arrancar un sistema operativo del menú de arranque.

- Si desea impedir además el arranque de uno o varios sistemas operativos del menú de arranque, añada la entrada `lock` a cada una de las secciones que no deba iniciarse sin introducir previamente la contraseña. Por ejemplo:

```
title linux
    kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
    initrd (hd0,4)/initrd
    lock
```

Así, después de reiniciar el sistema y seleccionar la entrada Linux en el menú de arranque, aparece el siguiente mensaje de error:

Error 32: Must be authenticated

Pulse **(Intro)** para acceder al menú y a continuación **(p)** para obtener un cursor en el que introducir la contraseña. Después de escribir la contraseña y pulsar **(Intro)**, se inicia el proceso de arranque del sistema operativo seleccionado (en este caso Linux).

Atención

Contraseña de arranque y pantalla de bienvenida

Al utilizar la contraseña de arranque en GRUB, no aparece la habitual pantalla de bienvenida.

Atención

Posibles problemas e información adicional

Atención

Problemas de arranque con GRUB

GRUB sólo comprueba la geometría de los discos duros conectados durante el arranque. En algunos casos excepcionales, los datos proporcionados por la BIOS pueden ser contradictorios y GRUB emite un "GRUB Geom Error". Si esto sucede, utilice LILO o actualice la BIOS si es necesario.

Atención

La página web <http://www.gnu.org/software/grub/> contiene abundante información sobre GRUB en alemán, inglés y japonés. el manual online está disponible sólo en inglés.

En caso de que `texinfo` esté instalado en su sistema, puede utilizar el comando `info grub` para ver en la shell las páginas de información sobre GRUB.

Arrancar con LILO

LILO el gestor de arranque de Linux, resulta idóneo para su instalación en el MBR. LILO tiene acceso a ambos discos duros en modo real y, ya desde su instalación, es capaz de encontrar todos los datos que necesita en los discos duros "crudos", sin tener información acerca de la partición. Es por eso que existe también la posibilidad de iniciar sistemas operativos desde el segundo disco duro. En comparación al proceso de arranque de DOS, se ignoran los datos en la tabla de particiones.

Pero la mayor diferencia respecto al arranque tipo DOS es la posibilidad de elegir entre diferentes sistemas operativos, siendo uno de ellos Linux. Después de la carga del MBR en la memoria RAM se ejecuta LILO, que le permite al usuario elegir de una lista de sistemas operativos instalados.

Durante el inicio es capaz de cargar y arrancar sectores de arranque de particiones, con el fin de arrancar un sistema operativo desde esa partición, o cargar un kernel de Linux para arrancar Linux. Además ofrece la posibilidad de pasar una línea de comando al kernel de Linux. Por razones de seguridad, los servicios de LILO pueden ser protegidos total o parcialmente por contraseña.

Fundamentos

La maquinaria de arranque de LILO se compone de las siguientes partes:

- *sector de arranque tipo LILO* con un comienzo del código de LILO ("primera fase") que activa el LILO real
- código máquina de LILO por lo general en: `/boot/boot - menu . b`
- *archivo map* (`/boot/map`), que genera LILO durante su instalación y que contiene información sobre la ubicación del kernel de Linux y de otros datos adicionales.
- opcional: el *archivo de mensaje* (`/boot/message`), que crea regularmente una selección de arranque gráfica.
- los distintos kernel de Linux y sectores de arranque, que LILO debe ofrecer para el arranque.

Aviso

¡Cualquier acceso de escritura y también el movimiento de alguno de estos componentes convierte el archivo map en no válido y pide por lo tanto una *reinstalación de LILO* (ver en la página 93)! Esto se refiere especialmente a cualquier cambio del kernel (p. ej. la actualización).

Aviso

El sector de arranque de LILO puede instalarse en los siguientes destinos:

En un *disquete*

Este es el método más fácil, pero a la vez el más lento, para arrancar con LILO. Escoja este método si no desea sobrescribir sobre el sector de arranque existente.

En el *sector de arranque* de una partición Linux primaria del primer disco duro
Esta variante no toca el MBR. Antes de arrancar hace falta marcar la partición con fdisk como activa. Para ello, escriba como root
`fdisk -s <Partition>`. fdisk le pregunta otra entrada; 'm' le proporciona una lista de las posibles entradas, y con 'a' se podrá arrancar desde la partición indicada.

(En el *Master Boot Record*)

Ésta es la variante que ofrece mayor flexibilidad. Se trata especialmente de la única posibilidad de arrancar Linux desde el disco duro, cuando todas las particiones de Linux se encuentran en el segundo disco y no hay ninguna partición extendida en el primero. No obstante, la modificación del MBR conlleva ciertos riesgos en caso de una instalación indebida.

Si se ha usado hasta ahora *otro gestor de arranque* ...

... y se quiere seguir usando el mismo, existen, dependiendo de sus prestaciones, un par de posibilidades adicionales. Un caso muy frecuente: Tiene una partición primaria en el segundo disco y desde allí quiere arrancar su SuSE Linux; suponiendo además que el "otro" gestor de arranque puede iniciar esa partición. En este caso puede hacerlo instalando LILO en el sector de arranque e indicando al otro gestor que la partición se puede arrancar.

Configuración de LILO

Como gestor de arranque flexible, LILO ofrece múltiples posibilidades para adaptarse a las necesidades individuales. A continuación se explican las op-

ciones más importantes; explicaciones más exhaustivas se encuentran en ?.

La configuración de LILO se graba en el archivo `/etc/lilo.conf`. Es aconsejable guardar bien el archivo de configuración de la última instalación de LILO y hacer una copia de seguridad antes de cualquier cambio. Ningún cambio se aplica si antes no se instala nuevamente LILO con la última versión del archivo de configuración (apartado *Instalar y desinstalar LILO* en la página 92)!

El contenido del archivo `lilo.conf`

El archivo `/etc/lilo.conf` comienza con un *apartado global* (ingl. *global options section*), con parámetros generales seguido de uno o varios *apartados de sistema* (ingl. *image sections*), para los distintos sistemas operativos que LILO debe arrancar. Cada nuevo apartado de sistema se introduce por la opción `image` o `other`.

El orden de aparición de los sistemas operativos en `lilo.conf` es importante por el hecho de que se arranca automáticamente el que aparece *primero*, en caso de que el usuario no intervenga. Esta intervención se puede realizar dentro de un tiempo de espera definido por las opciones `delay` o `timeout`.

El archivo 2 muestra una configuración de ejemplo para un ordenador con Linux y Windows. Al arrancar, se encontrará con las siguientes opciones definidas por este archivo: un kernel de Linux nuevo (`/boot/vmlinuz`), uno como solución de emergencia (`/boot/vmlinuz.suse`), MS-DOS (o Windows 95/98) en `/dev/hda1` y el programa Memtest86.

```
### LILO global section
boot      = /dev/hda           # LILO installation target: MBR
backup    = /boot/MBR.hda.990428 # backup file for the old MBR
                                   # 1999-04-28
vga        = normal           # normal text mode (80x25 chars)
read-only
menu-scheme = Wg:kw:Wg:Wg
lba32                      # Use BIOS to ignore
                                   # 1024 cylinder limit

prompt
password = q99iwr4          # LILO password (example)
timeout = 80                # Wait at prompt for 8 s before
                                   # default is booted
message = /boot/message     # LILO's greeting

### LILO Linux section (default)
  image = /boot/vmlinuz      # Default
  label = linux
```

```

root    = /dev/hda7          # Root partition for the kernel
initrd  = /boot/initrd

### LILO Linux section (fallback)
image   = /boot/vmlinuz.suse
label   = Fallsafe
root    = /dev/hda7
initrd  = /boot/initrd.suse
optional

### LILO other system section (Windows)
other   = /dev/hda1          # Windows partition
label   = windows

### LILO Memory Test)
image   = /boot/memtest.bin
label   = memtest86

```

Fichero 2: Configuración de ejemplo en /etc/lilo.conf

Todo lo que está en `/etc/lilo.conf` entre un símbolo `#` y el fin de la línea cuenta como comentario. LILO lo ignora igual que el espacio en blanco y usándolo se mejora la legibilidad. A continuación, repasamos brevemente las entradas imprescindibles; las opciones adicionales se describen en el apartado [El contenido del archivo lilo.conf](#) en la página anterior.

■ Sección global (Apartado de parámetros)

- `boot=<bootdevice>`

Dispositivo sobre el cual se debe instalar (en el primer sector) el sector de arranque de LILO (el destino de la instalación). `<bootdevice>` puede ser: una disquetera (`/dev/fd0`), una partición (p. ej. `/dev/hdb3`), o todo un disco (p. ej. `/dev/hda`): lo último significa la instalación en el MBR.

Configuración por defecto: Si falta este parámetro, LILO se instala en la partición raíz actual.

- `lba32`

Esta opción sobrepasa el límite de 1024 cilindros de LILO. Es algo que sólo funciona con el soporte apropiado de la BIOS.

- `prompt`

Fuerza la aparición del Prompt de LILO. ¡Por defecto no sale ningún prompt! (ver apartado [El contenido del archivo lilo.conf](#) en la página anterior, opción de `lay`).

Se recomienda ponerlo cuando LILO debe arrancar más de un sistema operativo. Junto con esta opción se debería definir también la opción `timeout` para que se pueda efectuar un reinicio automático cuando el usuario no introduce nada.

- `timeout=<décimas de segundo>`

Define un tiempo de selección y permite así un arranque automático, si no se selecciona nada.. *<décimas de segundo>* es el tiempo de que se dispone para realizar una entrada. Al pulsar (↑) esta función se desactiva y el ordenador se queda esperando una entrada. La configuración por defecto es 80.

■ Sección Linux

- `image=<kernel image>`

Aquí tiene que aparecer el nombre de la imagen del kernel a arrancar. Esto será por lo general `/boot/vmlinuz`.

- `label=<nombre>`

Un nombre para el sistema a libre elección pero fijo dentro de `/etc/lilo.conf` (p. ej. `linux`). La longitud máxima es de 15 caracteres; se permiten solo caracteres normales, cifras y "guión bajo" ('_'); no se permiten espacios o caracteres especiales como la ñ o la Ü, etc. Las reglas exactas para los caracteres permitidos se encuentran en ?, capítulo 3.2.1. El valor por defecto es el nombre de la imagen del kernel (p. ej. `/boot/vmlinuz`).

Con este nombre se selecciona el sistema operativo deseado y en caso de usar varios es recomendable proporcionar una explicación más detallada de los nombres y sistemas en un archivo de mensaje (ver apartado [El contenido del archivo lilo.conf](#) en la página 89, opción `message`).

- `root=<root device>`

Esta opción indica al kernel la partición root del sistema Linux (p. ej. `/dev/hda2`). ¡Se recomienda definirlo por seguridad! Sin esta opción el kernel toma la partición root que está anotada en él mismo.

- `append=<parameter>`

Si desea pasar a LILO posteriormente opciones de arranque adicionales para el kernel, añada al archivo `lilo.conf` una nueva línea que comience por `append` e introduzca los parámetros deseados después del signo `=` separados por un espacio y entrecomillados. Una vez realizados estos cambios, ejecute el comando `lilo` como usuario `root` para reinstalar LILO. Los cambios serán aplicados la próxima vez que inicie el sistema.

■ Apartado Linux [Linux – Ajustes seguros]

En caso de haber instalado un kernel propio, siempre es posible acceder a éste y arrancar el sistema.

- `optional`

Al borrar `/boot/vmlinuz.suse` (*no se recomienda!*), la instalación de LILO pasa por alto este apartado sin producir ningún mensaje de error.

■ Otro sistema

- `other=<partition>`

La variable `other` indica a LILO las particiones de arranque de otros sistemas para poder iniciarlos (p. ej. `/dev/hda1`).

- `label=<name>`

Escoja aquí un nombre para este sistema. La configuración por defecto – el mero nombre de dispositivo de la partición – no brinda mucha información.

■ Memory Test

Aquí sólo aparece el programa para el chequeo de memoria.

En este apartado se han comentado únicamente las entradas más significativas de `/etc/lilo.conf`. Puede encontrar más información sobre otras opciones de gran utilidad en la página del manual de `lilo.conf`, que se muestra con el comando `man lilo.conf`.

Instalar y desinstalar LILO

Aviso

Antes de instalar LILO asegúrese *siempre* de que los demás sistemas operativos disponibles pueden arrancarse con disquete (lo que no funciona en el caso de Windows XP). Sobre todo se tiene que poder usar `fdisk`. Si es necesario, SuSE Linux puede arrancarse también del CD o DVD de instalación.

Aviso

Instalar después de modificar la configuración

Si se ha cambiado alguno de los componentes de LILO (ver en la página 87) o si se ha modificado su configuración en `/etc/lilo.conf`, hace falta instalar LILO de nuevo. Esto se lleva a cabo iniciando el instalador map (*ingl. map-installer*) como usuario `root`:

```
/sbin/lilo
```

Primero LILO genera un backup del sector de arranque de destino, graba allí su "primera fase" y genera después un nuevo archivo map (ver en la página 87). LILO confirma en pantalla los sistemas instalados, lo que resulta para el ejemplo de arriba en el salida en pantalla:

```
Added linux *
Added suse
Added windows
Added memtest86
```

Una vez terminada la instalación, se puede arrancar el ordenador de nuevo (como usuario `root`):

```
shutdown -r now
```

Después del test de sistema de la BIOS, LILO muestra el prompt que permite pasar parámetros al kernel y elegir la imagen de arranque. Con `(Tab)` se pueden ver los nombres de las configuraciones instaladas.

Desinstalar el cargador de arranque de Linux

Para desinstalar GRUB o LILO se sobrescribe el sector de arranque donde está instalado el cargador de arranque Linux (GRUB o LILO) con su contenido *original*. En SuSE Linux esto no representa ningún problema *si* se dispone de una copia de seguridad válida. Utilice el módulo de cargador de arranque de YaST para crear una copia de seguridad del MBR original y volver a introducirla en el menú del cargador de arranque si es necesario, o bien crear un MBR estándar. Encontrará una descripción del módulo de cargador de arranque de YaST en la sección del *Manual de Usuario* dedicada a la instalación.

Aviso

La copia de seguridad de un sector de arranque deja de ser válida cuando la partición correspondiente ha recibido un nuevo sistema de archivos. La tabla de partición en un backup de MBR pierde completamente su validez cuando el disco ha sido reparticionado. Un backup de este estilo es una "bomba" que puede estallar en cualquier momento, por eso lo mejor es borrar backups caducados inmediatamente.

Aviso

Recuperar el MBR (DOS/Win9x/ME)

Para recuperar un MBR de DOS o Windows se utiliza el siguiente comando de MS-DOS (disponible a partir de la versión DOS 5.0 en adelante):

```
fdisk /MBR
```

o con el comando de OS/2:

```
fdisk /newmbr
```

Estos comandos solamente escriben los primeros 446 Bytes al MBR (el código de arranque) y dejan la tabla de partición sin tocar, salvo que el MBR (ver en la página 74) se encuentre como no válido por una "cifra mágica" falsa; en este caso se borra la tabla! *No olvide* activar con fdisk la partición de arranque, ya que las rutinas del MBR de DOS, Windows y OS/2 lo necesitan.

Recuperar el MBR (Windows XP)

Arranque con el CD de Windows XP y pulse la tecla (R) en el Setup para iniciar la consola de recuperación. A continuación seleccione de la lista su instalación de Windows XP e introduzca la contraseña del administrador. Introduzca en el prompt el comando FIXMBR y responda con y a la pregunta de confirmación. Finalmente, reinicie el ordenador con exit.

Recuperar el MBR (Windows 2000)

Arranque con el CD de Windows 2000 CD y pulse la tecla (R) en el Setup y la tecla (K) en el siguiente menú para iniciar la consola de recuperación. A continuación seleccione en la lista su instalación de Windows 2000 e introduzca la contraseña del administrador. Introduzca en el prompt el comando FIXMBR y responda con y a la pregunta de confirmación. Finalmente, reinicie el ordenador con exit.

Arrancar Linux después de recuperar el MBR

Una vez que ha restablecido el MBR estándar de Windows, puede volver a instalar el cargador de arranque de Linux de su elección para así poder seguir utilizando el sistema Linux instalado.

GRUB

Durante una instalación en el MBR, GRUB guarda una primera etapa o "stage1" en la partición Linux. Tras restablecer el MBR con YaST o con las herramientas Windows mencionadas en las líneas superiores, marque la partición Linux como activa por medio del programa fdisk. Para ello ejecute el comando `fdisk -s <particion>` como usuario root. A continuación, fdisk le pide que introduzca alguna instrucción. 'm' le proporciona una lista de las instrucciones disponibles. Con 'a' puede modificar la tabla de particiones de tal modo que sólo una partición primaria esté activa, es decir, la partición Linux con la copia stage1. Si es necesario compruébelo con el comando `p` (print) de fdisk.

LILO

Una vez recuperado el MBR de Windows, LILO puede volver a instalarse de una copia de seguridad existente. Compruebe que la copia de seguridad tiene el tamaño preceptivo de 512 bytes y vuélvalo a instalar utilizando los siguientes comandos:

- Si LILO está en la partición yyyy (p. ej. hda1, hda2,...):


```
dd if=/dev/yyyy of=nuevo-archivo bs=512 count=1
dd if=archivo-backup of=/dev/yyyy
```
- Si LILO está en el MBR del disco zzz (p. ej. hda, sda):


```
dd if=/dev/zzz of=nuevo-archivo bs=512 count=1
dd if=archivo-backup of=/dev/zzz bs=446 count=1
```

El último comando "tiene la precaución" de no modificar la tabla de particiones. Recuerde activar con fdisk la partición que debe formar ahora la de arranque.

Crear un CD de arranque

Debe crear un CD de arranque si tiene problemas al arrancar el sistema instalado con el gestor de arranque LILO, que ha configurado con ayuda de YaST. La creación de un disquete de arranque no funciona en las nuevas versiones de SuSE Linux, puesto que los archivos de arranque ya no caben en un disquete.

Procedimiento

Si su ordenador dispone de una grabadora, se puede crear un CD de arranque en el que queden grabados los archivos necesarios para el arranque.

Tenga en cuenta que se trata de un "rodeo". Por lo general debería ser posible configurar adecuadamente el gestor de arranque LILO. Eche un vistazo a la documentación que se encuentra en `/usr/share/doc/packages/lilo/README`, y a las páginas `man lilo.conf` y `man lilo`, que puede invocar con los comandos `man lilo.conf` y `man lilo`.

CD de arranque con ISOLINUX

La forma más sencilla de crear un CD de arranque es utilizar el gestor de arranque Isolinux. Con Isolinux también se puede convertir los CDs de instalación de SuSE en CDs de arranque.

- Arranque el sistema instalado de la siguiente forma (a partir de SuSE Linux 7.2):
 - Arranque con el CD o DVD de instalación, tal y como lo hizo en la instalación.
 - Escoja la opción 'Instalación' (por defecto).
 - Después escoja el idioma y la disposición del teclado.
 - En el siguiente menú, escoja el punto 'Arrancar sistema instalado'.
 - Se reconocerá automáticamente la partición root y el sistema arrancará.
- Instale el paquete `syslinux` con ayuda de YaST.
- Abra una shell como root. Con ayuda de los siguientes comandos se creará un directorio temporal para el CD, en el que copiará todos los archivos necesarios para el arranque del sistema Linux (el gestor de arranque Isolinux, así como el kernel y el `initrd`).

```
tierra:~ # mkdir /tmp/CDroot
tierra:~ # cp /usr/share/syslinux/isolinux.bin /tmp/CDroot/
tierra:~ # cp /boot/vmlinuz /tmp/CDroot/linux
tierra:~ # cp /boot/initrd /tmp/CDroot
```

- Ahora edite con su editor preferido el archivo de configuración del gestor de arranque `/tmp/CDroot/isolinux.cfg`. Cuando quiera utilizar p.ej. `pico`, invóquelo

```
pico /tmp/CDroot/isolinux.cfg
```

Introduzca el siguiente contenido:

```
DEFAULT linux
LABEL linux
    KERNEL linux
    APPEND initrd=initrd root=/dev/hdXY [bootparameter]
```

Introduzca en el parámetro `root=/dev/hdXY`, su partición de root. Si no está seguro de la descripción de la partición, la encontrará en el archivo `/etc/fstab`. Puede añadir otras opciones al valor `[bootparameter]` que se utilizarán al arrancar. Los archivos de configuración serán algo parecido a esto:

```
DEFAULT linux LABEL linux KERNEL linux APPEND initrd=initrd
root=/dev/hda7 hdd=ide-scsi
```

- Finalmente se creará un sistema de archivos ISO9660 para el CD sacado de los archivos con la siguiente orden (escriba todo el comando en la misma línea):

```
mkisofs -o /tmp/bootcd.iso -b isolinux.bin -c boot.cat
    -no-emul-boot -boot-load-size 4
    -boot-info-table /tmp/CDroot
```

Compruebe que toda la orden se encuentra dentro de la misma línea

- Ahora se puede grabar el archivo `/tmp/bootcd.iso` en el CD, ya sea con un programa gráfico como KonCD o XCDroast, o desde la línea de comandos:

```
cdrecord -v speed=2 dev=0,0,0 /tmp/bootcd.iso -eject
```

Eventualmente el parámetro `dev=0,0,0` deberá adecuarse al ID SCSI de la grabadora (lo que puede comprobar mediante la entrada del comando `cdrecord -scanbus`, o también en la página del manual de `cdrecord` (`man cdrecord`)).

- ¡Pruebe el CD de arranque! Para ello reinicie el ordenador y compruebe si su sistema Linux arranca correctamente desde el CD.

El sistema X Window

El sistema X Window o X Window System es prácticamente un estándar para entornos gráficos de usuario en Unix. Pero sistema X Window, denominado también X11, es todavía mucho más: es un sistema basado en redes. Las aplicaciones que estén funcionando en el ordenador *tierra* pueden mostrar sus salidas en pantalla en el ordenador *so*l si ambas máquinas están conectadas a través de una red. Esta red puede ser una LAN (Local Area Network – red de área local), pero también es posible que los ordenadores se encuentren separados por miles de kilómetros de distancia y se comuniquen entre sí por medio de Internet.

A continuación le presentamos, entre muchas otras cosas, al programam `xf86config`, que puede emplearse para configurar monitor, tarjeta gráfica, teclado y ratón como alternativa al programa `SOX2` . También se explicará la configuración 3D de OpenGL. La descripción de los módulos de `YOST` está incluida en ?.

Historia de XFree86	100
La versión 4.x de XFree86	101
Configuración con <code>xf86config</code>	102
Optimizar la instalación del sistema X Window	111
Configuración de OpenGL/3D	120

Historia de XFree86

X11 se desarrolló gracias a la cooperación entre DEC (Digital Equipment Corporation) y el proyecto Athena del MIT (Massachusetts Institute of Technology). La primera versión (X11R1) salió en septiembre de 1987. Desde la versión 6 (Release 6) la X Consortium, Inc., y desde 1996 The Open Group, acogieron el desarrollo del X Window System.

XFree86™ es una implementación libre de servidores X para sistemas Unix a base de PC (ver <http://www.XFree86.org>). XFree86 se sigue desarrollando por programadores en todo el mundo, que se unieron en 1992 para formar el XFree86-Team. De esta unión surgió en 1994 la empresa The XFree86 Project, Inc. cuyo objetivo es poner XFree86™ a la disposición de un amplio público y contribuir con el desarrollo e investigación del sistema X Window. Desde marzo del 2000 existe la versión XFree86 4.x, que está completamente actualizada. SuSE Linux incorpora por defecto XFree86 4.0, cuyas características se explican un poco más adelante.

Los siguientes apartados se ocupan de la configuración del servidor X. Con este fin se explica `xf86config`, una aplicación que puede utilizarse como alternativa a `SoX2` para configurar el sistema X Window.

Para usar el hardware existente (ratón, tarjeta de vídeo, monitor, teclado) de la mejor forma, existe la posibilidad de optimizar la configuración a mano; solamente se discutirán los aspectos más importantes de esta optimización manual. Varios ficheros del directorio `/usr/share/doc/packages/xf86` al igual que la página del manual de `XF86Config` (`man XF86Config`) contienen información adicional sobre el sistema X Window.

Aviso

Se recomienda mucha precaución a la hora de configurar el sistema X Window. Jamás se debe arrancar X sin haber terminado la configuración. Un sistema mal ajustado puede provocar daños irreparables al hardware; los monitores de frecuencia fija corren un riesgo especial. Los autores de este libro y SuSE Linux AG no se responsabilizan de posibles daños. El presente texto fue redactado con máximo cuidado, no obstante, no se puede garantizar que los métodos presentados sean correctos para su hardware y que no pueda causarles daño.

Aviso

La versión 4.x de XFree86

SuSE Linux incorpora ahora la versión 4.x de XFree86, que se diferencia en algunos aspectos de la versión 3.3, incorporada anteriormente. Para el usuario solo existen pequeñas diferencias; los entornos gráficos como p. ej. GNOME y KDE se comportan igual a la versión 3.3.6 de XFree86.

¿Cuáles son las ventajas de esta versión?

El nuevo servidor X ya no es un programa "monolítico", sino que ahora existe una base relativamente pequeña sobre la que se cargan módulos adicionales según la necesidad. Por ejemplo, ya no existen servidores X especiales para las diferentes tarjetas gráficas; ahora existe un único ejecutable con nombre XFree86 que se encuentra en `/usr/X11R6/bin`. Este representa el servidor X y el driver que se encarga de la comunicación con la tarjeta es un módulo que se puede cargar.

El soporte de diferentes dispositivos, fuentes o protocolos se realiza en la misma forma con módulos que se cargan en tiempo de ejecución. Normalmente no hace falta preocuparse de esto ya que `SeqX2` se encarga en gran medida de la configuración de los módulos necesarios para el entorno gráfico.

Debido al concepto de módulos, es mucho más fácil para los fabricantes de hardware, desarrollar un driver p. ej. para una pantalla táctil o una tarjeta gráfica muy nueva. Incluso los desarrolladores de XFree86 procuraron la compatibilidad entre diferentes sistemas operativos. Un driver para una determinada tarjeta gráfica que fue compilado bajo FreeBSD se puede usar también en Linux y vice versa. Esta portabilidad se restringe evidentemente a una determinada plataforma; un módulo compilado para Linux en PowerPC, no se puede usar en un PC con instrucciones x86 (AMDs, Cyrix, Intel, etc.).

Además el soporte del ratón fue mejorado, lo que representa una respuesta más rápida cuando la máquina está muy cargada. En general todo el apartado gráfico funciona con más rapidez, debido sobre todo a la arquitectura de aceleración gráfica XAA mejorada (ingl. *XFree86 Acceleration Architecture*).

El fichero de configuración es un poco diferente, en comparación a XFree86 3.3.x. Para ajustar el servidor X en detalle, se recomienda consultar las explicaciones de la sintaxis del fichero de configuración que se encuentran en el apartado *Optimizar la instalación del sistema X Window* en la página 111. El fichero de configuración se encuentra ahora en `/etc/X11/XF86Config`. Otra mejora es el registro de errores que se encuentra ahora en `/var/log/XFree86.0.log`.

Una característica adicional de esta versión es el soporte de opciones especiales como p. ej. fuentes "true type", el soporte de la extensión del protocolo 3D `glx`,

corrección gamma del monitor y el soporte de varias tarjetas gráficas para una configuración **Multihead**. Puede encontrar información detallada en el apartado *Optimizar la instalación del sistema X Window* en la página 111.

¿Qué ha cambiado?

XFree86 4.x está basado en la versión anterior 3.3.x. Desafortunadamente no ha sido posible portar todos los drivers a la nueva versión, ya que algunos son muy complejos y el cambio a la arquitectura XAA es otro obstáculo para algunos drivers. Estas tarjetas gráficas siguen siendo soportadas por XFree86 3.3.6 y se configuran igual que antes mediante **SaX**.

En particular se trata de tarjetas gráficas que fueron soportadas por medio de los siguientes servidores X: **XF86_S3**, **XF86_Mach8**, **XF86_Mach32** y **XF86_8514**. En cuanto a las tarjetas **S3**, significa que todas las tarjetas que necesitan el servidor **S3** no están soportadas por XFree86 4.0; en cambio, las tarjetas **S3** soportadas por el servidor **SVGA** funcionan con XFree86 4.0; estas tarjetas son aquellas con chip **S3 Trio3D**, **Savage4**, **Savage3D**, **Savage2000** y casi todas las tarjetas **S3 Virge**.

Las tarjetas que necesitan los servidores **X Mach8**, **Mach32** o **8514** ya no se usan mucho y están – al igual que las tarjetas antiguas del tipo **S3** – soportadas por medio de XFree86 3.3.x.

Configuración con **xf86config**

SaX como herramienta de configuración supera casi siempre al programa **xf86config** cuando se trata de configuraciones simples del sistema **X Window**. En las pocas ocasiones en las que **SaX** no llega a configurar correctamente el servidor **X**, esto funciona casi siempre con **xf86config**.

También para XFree86 4.x existe un programa de configuración a base de pantallas de texto (**xf86config**). La diferencia principal radica en que por una parte tiene algunos diálogos ligeramente cambiados y por otra guarda el fichero de configuración en **/etc/X11/XF86Config**.

Por lo tanto, la siguiente descripción se refiere exclusivamente al programa **xf86config** de XFree86 3.3.x.

En el caso de XFree86 4.x, la utilización de **xf86config** no es necesaria en la mayoría de los casos, ya que aquí las tarjetas gráficas “problemáticas” también pueden configurarse con el **framebuffer** o el módulo **vga**.

Para la configuración se necesita una serie de datos:

- Tipo de ratón, puerto de conexión y velocidad de transferencia en baudios (lo último suele ser opcional).
- Especificación de la tarjeta de vídeo.
- Especificación del monitor (frecuencias, etc.).

Conociendo estos datos se puede comenzar con la configuración, que solamente puede ser ejecutada por el usuario `root`.

La configuración se inicia con:

```
tierra:/root # xf86config
```

Ratón

Después de una pantalla de bienvenida, el primer menú pregunta por el tipo de ratón. Aparecen las siguientes opciones:

1. Microsoft compatible (2-button protocol)
2. Mouse Systems (3-button protocol)
3. Bus Mouse
4. PS/2 Mouse
5. Logitech Mouse (serial, old type, Logitech protocol)
6. Logitech MouseMan (Microsoft compatible)
7. MM Series
8. MM HitTablet

Mensaje en pantalla 4: Selección de ratón para las X

Configurando el tipo de ratón hay que considerar que, muchos de los ratones más recientes de Logitech son compatibles con Microsoft o que usan el protocolo MouseMan. ¡La selección de `BUS Mouse` se refiere a todos los tipos de ratón de bus, también los de Logitech!

El tipo de ratón adecuado se selecciona indicando el número al comienzo de la fila. Después (p. ej. seleccionando el tipo 1) aparece la pregunta por la activación de `ChordMiddle`. Se trata de una opción necesaria para la activación del botón del medio de algunos ratones de Logitech o para algunos Trackballs:

```
Please answer the following question with either 'y' or 'n'.
Do you want to enable ChordMiddle?
```

La afirmación ('y') de la siguiente pregunta permite la emulación de un tercer botón de ratón para aquellos que solo tienen dos botones:

Please answer the following question with either 'y' or 'n'.
Do you want to enable Emulate3Buttons?

Para emular el tercer botón del ratón hay que pulsar simultáneamente los dos botones.

Después se pregunta por el puerto en el cual está el ratón:

Now give the full device name that the mouse is connected to, for example /dev/tty00. Just pressing enter will use the default, /dev/mouse. Mouse device:

Durante la instalación ya se ha definido un puerto de ratón, así que se puede usar aquí esta definición (/dev/mouse).

Teclado

Ahora viene la pregunta, si se debería asignar a la tecla izquierda de **(Alt)** el valor Meta (ESC) y a la derecha de **(Alt)** el valor ModeShift (AltGr):

Please answer the following question with either 'y' or 'n'.
Do you want to enable these bindings for the Alt keys?

Es aconsejable elegir 'y' para llegar a los caracteres especiales que se alcanzan con **(Alt Gr)** y también para poder usar la tecla izquierda de **(Alt)** como Meta-tecla – especialmente práctico cuando se usa Emacs.

Monitor

Ahora hay que especificar el monitor. Los datos críticos son la frecuencia vertical y horizontal que están generalmente documentados en el manual del monitor.

Aviso

¡Indicar rangos de frecuencia equivocados puede provocar la destrucción del monitor! El sistema X Window solo usa los modos de vídeo que envían señales localizadas dentro del rango de frecuencias admitidas.

Aviso

Los valores admisibles para algunos monitores se encuentran en /usr/X11R6/lib/X11/doc/monitors. ¡No hay garantía para estos valores!

Para elegir la frecuencia horizontal se presenta la siguiente selección:

```
hsync in kHz; monitor type with characteristic modes
1 31.5;                      Standard VGA, 640x480 @ 60 Hz
2 31.5 - 35.1;               Super VGA, 800x600 @ 56 Hz
```

```

3 31.5, 35.5;      8514 Compatible, 1024x768 @ 87 Hz interl.
                   (no 800x600)
4 31.5, 35.15, 35.5; Super VGA, 1024x768 @ 87 Hz il.,
                   800x600 @ 56 Hz
5 31.5 - 37.9;     Extended Super VGA, 800x600 @ 60 Hz,
                   640x480 @ 72 Hz
6 31.5 - 48.5;     Non-Interlaced SVGA, 1024x768 @ 60 Hz,
                   800x600 @ 72 Hz
7 31.5 - 57.0;     High Frequency SVGA, 1024x768 @ 70 Hz
8 31.5 - 64.3;     Monitor that can do 1280x1024 @ 60 Hz
9 31.5 - 79.0;     Monitor that can do 1280x1024 @ 74 Hz
10 Enter your own horizontal sync range
Enter your choice (1-10):

```

Mensaje en pantalla 5: Definición de las frecuencias horizontales del monitor

Sólo en caso de no conocer los datos exactos del monitor, se escogerá una de las opciones predefinidas. Con '10' es posible introducir las frecuencias exactas.

Después del diálogo que pregunta por las frecuencias horizontales hay que definir las verticales. Aquí se presenta también una selección:

```

1 50-70
2 50-90
3 50-100
4 40-150
5 Enter your own vertical sync range

```

Enter your choice (1-5):

Mensaje en pantalla 6: Frecuencias verticales detalladas

Como en la anterior pregunta, es mejor introducir los valores exactos en lugar de recurrir a uno de los rangos dados de '1' a '4'.

Después se pide introducir un nombre para la descripción del monitor,

Enter an identifier for your monitor definition:

el nombre del fabricante,

Enter the vendor name of your monitor:

y el modelo:

Enter the model name of your monitor:

En las anteriores preguntas se puede introducir el nombre correspondiente o usar los valores predeterminados pulsando **(Intro)**. Con esto se finaliza la especificación del monitor.

Tarjeta gráfica/servidor X

Se continúa con la especificación de la tarjeta gráfica usada:

Do you want to look at the card database?

Introduciendo 'y' aparece una lista con tarjetas de vídeo preconfiguradas.

Se puede seleccionar de esta lista la definición de una tarjeta indicando el número correspondiente. ¡Al elegir una tarjeta gráfica hay que tener en cuenta que incluso tarjetas del mismo tipo pueden tener variaciones respecto a Clock-Chip y RAMDAC (ingl. *Random Access Memory Digital-to-Analogue Converter*)!

Por eso existe más adelante la opción de configurar Clock-Chip y RAMDAC de manera individual, aunque la tarjeta ya haya sido elegida anteriormente de la lista de preconfiguraciones.

Las definiciones de la base de datos de tarjetas, contienen información sobre Clock-Chip, RAMDAC y el servidor X a usar. Según el caso, se añaden también datos interesantes sobre la tarjeta en la sección Device del fichero XF86Config.

Si la tarjeta gráfica buscada no se encuentra en el listado, no hay por qué preocuparse. Es posible volver con 'q' a la configuración normal. Al seleccionar una tarjeta, solamente se debería seleccionar una del listado, cuando el nombre de la lista corresponde exactamente con la tarjeta usada. No se recomienda elegir una tarjeta con un nombre parecido, ya que esto no significa que el hardware también lo sea.

En el apartado *Optimizar la instalación del sistema X Window* en la página 111 hay información adicional sobre la configuración de la tarjeta gráfica.

Después de haber especificado la tarjeta viene la selección del servidor X:

- 1 The XF86_Mono server. This a monochrome server that should work on any VGA-compatible card, in 640x480 (more on some SVGA chipsets).
- 2 The XF86_VGA16 server. This is a 16-color VGA server that should work on any VGA-compatible card.
- 3 The XF86_SVGA server. This is a 256 color SVGA server that supports a number of SVGA chipsets. It is accelerated on some Cirrus and WD chipsets; it supports 16/32-bit color on certain Cirrus configurations.
- 4 The accelerated servers. These include XF86_S3, XF86_Mach32, XF86_Mach8, XF86_8514, XF86_P9000, XF86_AGX, XF86_W32 and XF86_Mach64.

These four server types correspond to the four different "Screen" sections in XF86Config (vga2, vga16, svga, accel).

- 5 Choose the server from the card definition, XF86_S3.

Which one of these four screen types do you intend to run by default (1-4)?

Mensaje en pantalla 7: Selección del servidor X

- 1 Un servidor para monitores monocromáticos. Debería funcionar con cualquier tarjeta gráfica compatible a VGA con una resolución mínima de 640x480 puntos.
- 2 El servidor de 16 colores XF86_VGA16. Debería funcionar con cualquier tarjeta compatible a VGA.
- 3 El servidor SVGA XF86_SVGA. Este servidor de 256 colores soporta una gran cantidad de tarjetas SVGA. Algunas tarjetas de Cirrus y de WD aprovechan la aceleración de gráficos. Hay tarjetas de Cirrus que permiten una profundidad de color 16 o 32-Bit en modo color.
- 4 Servidor para tarjetas aceleradoras. Hay varios servidores disponibles (ver más abajo)
- 5 Esta opción solo existe cuando se ha elegido una tarjeta en la lista anterior. Se propone el servidor adecuado para la tarjeta.

Cuando se ha elegido un servidor, aparece una pregunta acerca de la generación de un enlace simbólico del servidor elegido en `/usr/X11R6/bin/X`. Al afirmar la pregunta con 'y', el programa pide la confirmación para colocar el enlace en `/var/X11R6/bin`:

Do you want to set it in `/var/X11R6/bin`?

Afirme esta pregunta, porque es posible que no necesariamente se pueda escribir en el árbol `/usr`.

Ahora aparece un menú con los servidores X disponibles para tarjetas aceleradoras, si en la selección anterior se ha escogido '4':

Select an accel server:

- 1 XF86_S3
- 2 XF86_Mach32
- 3 XF86_Mach8
- 4 XF86_8514
- 5 XF86_P9000
- 6 XF86_AGX
- 7 XF86_W32
- 8 XF86_MACH64

Which accel server:

Estos servidores son especiales y soportan las prestaciones adicionales de las correspondientes tarjetas. La colocación del enlace supone que el servidor X correcto ya fue instalado durante la instalación del sistema X Window.

Después de la selección del servidor X, hace falta especificar la tarjeta gráfica en más detalle. Primero se define la cantidad de memoria instalada.

How much video memory do you have on your video card:

- 1 256K
- 2 512K
- 3 1024K
- 4 2048K
- 5 4096K
- 6 Other

Enter your choice:

Mensaje en pantalla 8: Definición de la cantidad de memoria gráfica

Después pregunta por un nombre, el fabricante y el tipo de tarjeta gráfica. Si se ha elegido antes la tarjeta desde la base de datos es suficiente con pulsar .

Enter an identifier for your video card definition:

Enter the vendor name of your video card:

Enter the model (board) name of your video card:

Si se ha elegido como servidor X uno del tipo acelerado, aparece ahora la pregunta por el "RAMDAC-Setting". Solo es importante para tarjetas tipo S3 o AGX:

1	AT&T 20C490 (S3 server)	att20c490
2	AT&T 20C498/21C498/22C498 (S3)	att20c498
3	AT&T 20C505 (S3)	att20c505
4	BrookTree BT481 (AGX)	bt481
5	BrookTree BT482 (AGX)	bt482
6	BrookTree BT485/9485 (S3)	bt485
7	Sierra SC15025 (S3, AGX)	sc15025
8	S3 GenDAC (86C708) (autodetected)	s3gendac
9	S3 SDAC (86C716) (autodetected)	s3_sdac
10	STG-1700 (S3)	stg1700
11	TI 3020 (S3)	ti3020
12	TI 3025 (S3)	ti3025

13	TI 3020 (S3, autodetected)	ti3020
14	TI 3025 (S3, autodetected)	ti3025
15	TI 3026 (S3, autodetected)	ti3026
16	IBM RGB 514 (S3, autodetected)	ibm_rgb514
17	IBM RGB 524 (S3, autodetected)	ibm_rgb524
18	IBM RGB 525 (S3, autodetected)	ibm_rgb525
19	IBM RGB 526 (S3)	ibm_rgb526
20	IBM RGB 528 (S3, autodetected)	ibm_rgb528
21	ICS5342 (S3, ARK)	ics5342
22	ICS5341 (W32)	ics5341
23	IC Works w30C516 ZoomDac (ARK)	zoomdac
24	Normal DAC	normal

Mensaje en pantalla 9: Indicación del RAMDAC

Generalmente lo mejor es pulsar  y no seleccionar nada, salvo que se haya elegido una tarjeta que soporta una configuración de RAMDAC especial. Este caso estará indicado y se recomienda seleccionarlo realmente.

Después de haber contestado a esto se puede elegir el Clock-Chip de las tarjetas aceleradas si es que lo llevan. Seleccionando un Clock-Chip ya no se necesitan líneas de Clock, ya que los valores Clock necesarios pueden ser programados:

1	Chrontel 8391	ch8391
2	ICD2061A and compatibles (ICS9161A, DCS2824)	icd2061a
3	ICS2595	ics2595
4	ICS5342 (similar to SDAC, but not completely compatible)	ics5342
5	ICS5341	ics5341
6	S3 GenDAC (86C708) and ICS5300 (autodetected)	s3gendac
7	S3 SDAC (86C716)	s3_sdac
8	STG 1703 (autodetected)	stg1703
9	Sierra SC11412	sc11412
10	TI 3025 (autodetected)	ti3025
11	TI 3026 (autodetected)	ti3026
12	IBM RGB 51x/52x (autodetected)	ibm_rgb5xx

Mensaje en pantalla 10: Determinación del Clockchip

Si se usa una tarjeta gráfica sin "Clock-Chip", es suficiente con pulsar  para no seleccionar ninguno. Si la tarjeta fue seleccionada en el listado de tarjetas se indica automáticamente el Clock-Chip que exista.

Sin haber seleccionado ningún Clock-Chip, xf86config propone iniciar el programa X -probeonly para determinar los Clock-Timings que soporta la tarjeta. Estos se apuntarán automáticamente en una línea de CLOCKS en el fichero XF86Config.

Aquí hay que indicar claramente, por qué los Clock-Timings que se determinan automáticamente pueden ser **muy peligrosos**: Si la tarjeta tiene un Clock-Chip programable, el servidor X no puede cambiar entre los distintos Clocks de la tarjeta y por tanto solo reconoce los Clocks 0, 1 y a veces 2. Los demás valores son más o menos casuales (generalmente los Clocks 0, 1 y 2 se repiten y por eso se reemplazan por ceros).

Los clocks distintos de 0 y 1 dependen mucho de la pre-programación del Clock-Chip, por lo que el valor del Clock 2 puede ser diferente cuando se efectúa la prueba (valor que se apunta en XF86Config) al valor del momento de arrancar el servidor X. De este modo todos los Timings son falsos y el monitor se puede dañar.

Un buen indicio para un Clock-Chip programable y sus problemas son muchos ceros en los valores del Timing o valores que continuamente se repiten. ¡En ningún caso se deben introducir valores semejantes en el fichero XF86Config!

Para determinar el Clock-Chip o el Clock-Timing se puede usar la siguiente estrategia:

- Lo mejor es indicar un **Clock-Chip programable** si es que existe sobre la tarjeta. En este caso se programa correctamente y el fichero XF86Config no contendría ninguna referencia a los Clocks. Otra posibilidad es la comparación de los circuitos (chips) que hay sobre la tarjeta con los Clock-Chips que se ofrecen en el menú, para averiguar así el que coincide. Casi todas las tarjetas modernas del tipo S3 llevan un Clock-Chip programable.
- Si no tiene **ningún Clock-Chip programable** sobre la tarjeta, lo mejor es ejecutar X -probeonly y comparar los valores encontrados con los del manual de la tarjeta (en el ordenador no debe funcionar ningún otro programa). Si estos más o menos coinciden (± 2), anote los valores en el fichero XF86Config.

Si no es posible comparar los valores, compruebe la validez de los mismos (muchos ceros o valores que se repiten continuamente indican valores no válidos). Anote los valores válidos a mano en XF86Config, pero no suprima ningún valor ni intente reordenar o modificar de alguna manera los mismos. Hay que apuntar los valores en el mismo orden de aparición.

Usando el servidor P9000 se introduce sencillamente, para cada modo, el clock deseado en la línea Clocks. El orden de los modos no es importante.

- Siempre es válido: Cuando el Clock-Chip es programable no debe existir ninguna línea de Clocks en XF86Config (Excepción: P9000).

Al contrario, cuando el Clock-Chip *no* es programable, sí que debe haber una línea de `Clocks` en `XF86Config`. Así se evita la determinación automática pesada y tal vez peligrosa de los `Clocks` en cada arranque del sistema X Window. Además en caso de tarjetas que no permiten leer los `Clocks` no aparecen valores falsos y así no habrá riesgo para el monitor.

Para probar ahora los `Clocks` (tenga en cuenta los párrafos anteriores), se contesta la siguiente pregunta con 'y':

Do you want me to run 'X -probeonly' now?

La pantalla se oscurece por un momento y después aparece una lista con los `Clocks` determinados o, un mensaje advirtiéndolo que no se ha encontrado ningún `Clock`. Si se ha definido un `Clock-Chip` con anterioridad no aparece la pregunta sobre ejecutar `X -probeonly`, ya que los `Clocks` se programarán automáticamente. En este caso aparece directamente la próxima opción de configuración.

Aviso

¡Si ha contestado la última pregunta con 'y' y la pantalla se queda oscura por más de 30 segundos, debe terminar en todo caso la fase de prueba con `(Control) + (Alt) + (←)` o `(Control) + (C)`! Si no queda más remedio apague el monitor y el ordenador para no poner en peligro estos componentes.

Aviso

Guardar la configuración

Ahora se ha terminado la configuración pero el fichero de configuración aún no está guardado. Lo mejor es guardar el fichero de configuración de X-Window `XF86Config` en el directorio `/etc`. Así se asegura también en una red que cada ordenador lleve su "propia" configuración, incluso cuando varios ordenadores comparten el árbol `/usr`.

Indique entonces `'/etc/XF86Config'` como destino del fichero de configuración. Con esto se termina el programa `xf86config` y la configuración del sistema X Window.

Optimizar la instalación del sistema X Window

A continuación se presenta la sintaxis del fichero de configuración `/etc/X11/XF86Config`. El fichero se divide en secciones que comienzan con la palabra

clave `Section` "nombre" y terminan con `EndSection`. Estas secciones se explican a grandes rasgos en este apartado.

Además se explica cómo añadir fuentes adicionales, cómo configurar los dispositivos de entrada y cómo realizar la aceleración 3D. Todas estas configuraciones se realizan en determinadas secciones dentro de `XF86Config`. Añadir una fuente adicional requiere la ayuda de programas externos que están incluidos en SuSE Linux y que forman parte de la instalación por defecto. Los procedimientos que se detallan aquí demuestran las capacidades principales, sin pretender ser exhaustivos pero que en cambio sirvan de ejemplo.

Los programas `SaX2` y `xf86config` (para XFree86 4.x) generan el fichero `XF86Config` y lo copian generalmente en el directorio `/etc/X11`. Este es el fichero de configuración principal del X Window System que contiene las definiciones de ratón, monitor y tarjeta de vídeo.

`XF86Config` se compone de varios párrafos llamados "secciones" (ingl. *sections*) y cada una contempla un determinado aspecto de la configuración. Cada sección tiene la forma:

```
Section <Denominador de sección>
    definición 1
    definición 2
    definición n
EndSection
```

Existen los siguientes tipos de secciones:

Files	Esta sección describe las rutas para los juegos de caracteres y la tabla de colores RGB.
ServerFlags	Aquí se apuntan indicadores generales (ingl. <i>flags</i>).
InputDevice	Esta es la sección de configuración de los dispositivos de entrada. En comparación a XFree86 3.3 se configuran teclados y ratones así como dispositivos especiales como Joysticks, tabletas digitalizadoras, etc. Las variables importantes aquí son <code>Driver</code> y las opciones <code>Protocol</code> y <code>Device</code> para determinar el protocolo y el dispositivo.

Cuadro 5.1: Continúa en la página siguiente...

Monitor	Descripción del monitor usado. Los elementos de esta sección son un nombre, que sirve más adelante de referencia en la definición del <code>Screen</code> , así como el valor de la anchura de banda (<code>Bandwidth [MHz]</code>) y de las frecuencias de sincronización permitidas (<code>HorizSync [kHz]</code> y <code>VertRefresh [Hz]</code>). El servidor "rechaza" cualquier <code>Modeline</code> que no cumple con la especificación del monitor; de esta forma se evita enviar al monitor frecuencias demasiado altas cuando se están manipulando los <code>Modelines</code> .
Modes	Aquí se definen los parámetros para las determinadas resoluciones de pantalla. <code>SOX2</code> calcula estos parámetros en base a las indicaciones por parte del usuario y por lo general no se requiere ninguna modificación. Se puede realizar una intervención manual p. ej. en caso de usar un monitor con frecuencia fija. La explicación exacta de todos los parámetros se encuentra en el fichero <code>HOWTO /usr/share/doc/howto/en/XFree86-Video-Timings-HOWTO.gz</code> , ya que para este libro resultaría demasiado extenso.
Device	Esta sección define una determinada tarjeta gráfica cuya referencia es el nombre que aparece por detrás de la palabra clave <code>Device</code> .
Screen	Esta sección une finalmente un <code>Driver</code> con un <code>Device</code> para formar así las indicaciones necesarias para <code>XFree86</code> . La sub-sección <code>Display</code> permite la definición de un tamaño de pantalla virtual (<code>Virtual</code>), del <code>Viewport</code> y de los <code>Modes</code> usados con este <code>Screen</code> .
ServerLayout	Esta sección define el diseño de una configuración con uno o varios monitores ("single" o "multihead"). Los dispositivos de entrada <code>InputDevice</code> y los monitores <code>Screen</code> se unen para formar un conjunto.

Cuadro 5.1: Secciones ("sections") en `/etc/X11/XF86Config`

A continuación se contemplan más de cerca las secciones `Monitor`, `Device` y `Screen`. En la página del manual de `XF86Config` (`man XF86Config`) y en la página del manual de `XF86Config` (`man XF86Config`) hay más información sobre las demás secciones.

En el fichero `XF86Config` pueden aparecer varias secciones de los tipos

Monitor y Device. También se pueden usar varias secciones Screen dependiendo su uso de la siguiente sección ServerLayout.

Sección Screen

Primero queremos tratar de cerca la sección de Screen. Esta une una sección de Monitor y de Device y determina qué resolución es proporcional con qué profundidad de color.

Una sección del tipo Screen puede parecerse p. ej. a la del fichero 3.

```
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
```

Fichero 3: La sección Screen del fichero /etc/X11/XF86Config

La línea Identifier (en este ejemplo el identificador es Screen[0]) da un nombre único a la sección para poder referenciar esta sección de forma inequívoca en la siguiente sección ServerLayout.

La tarjeta gráfica y el monitor definido se asignan mediante las líneas Device y Monitor a la pantalla Screen. No son más que referencias a las secciones de dispositivo (Device) y Monitor con los nombres correspondientes o identificadores "Identifier". Estas secciones se explican más adelante.

La variable DefaultColorDepth indica la profundidad de color por defecto que usa el servidor cuando arranca sin definición explícita de ella.

Para cada profundidad de color prosigue una subsección de `Display`. La profundidad de color de cada subsección se define por la palabra clave `Depth`. Los valores posibles para `Depth` son 8, 15, 16, 24 y 32 bpp. No todos los módulos de servidor X soportan todos los valores y, 24 y 32 dan como resultado la misma profundidad de color. 24bpp representa el modo "packed-pixel" y 32bpp el modo "padded-pixel".

Después de definir la profundidad de color se define con `Modes` una lista de resoluciones; el servidor X pasa por esta lista de izquierda a derecha. Para cada una de las resoluciones listadas, el servidor busca en la sección `Modes` un `Modeline` que corresponda a las capacidades gráficas del monitor y de la tarjeta gráfica.

La primera resolución adecuada en este sentido es la que usa el servidor X para arrancar el "Default -Mode". Con las teclas `(Control) + (Alt) + (gris +)` se puede ir en la lista de resoluciones a la derecha y con `(Control) + (Alt) + (gris -)` a la izquierda¹. Así se puede modificar la resolución en pantalla durante el tiempo de ejecución del sistema X Window.

La última línea de la subsección `Display` con la expresión `Depth 16` se refiere al tamaño de la pantalla virtual. El tamaño máximo de la pantalla virtual depende de la cantidad de memoria instalada y de la profundidad de color deseada pero no depende de la resolución máxima del monitor. Como las tarjetas gráficas modernas ofrecen mucha memoria, se pueden crear escritorios virtuales muy grandes. En tal caso es posible que ya no se pueda aprovechar la aceleración 3D, por haber ocupado toda la memoria de vídeo con un escritorio virtual. Si la tarjeta tiene p. ej. 16 MB Vídeo RAM, entonces la pantalla virtual puede ser de hasta 4096x4096(!) puntos a una profundidad de color de 8 Bit. Para los servidores X acelerados no se recomienda de ninguna manera usar todo el espacio de memoria disponible para la pantalla virtual, ya que estos servidores usan la zona de memoria no usada de la tarjeta para diferentes cachés de juegos de caracteres y de zonas de gráficos.

Sección Device

Una sección de dispositivo (ingl. *Device-Section*), describe una determinada tarjeta gráfica. Puede existir una cantidad infinita de secciones de dispositivo en `XF86Config` mientras que sus nombres, indicados con la palabra clave `Identifier`, se distinguen. Si hay varias tarjetas gráficas montadas en la máquina, estas secciones reciben números consecutivos comenzando con `Device[0]` para la primera, `Device[1]` para la segunda, etc. El siguiente fichero muestra el extracto de una sección del tipo `Device` de un ordenador con una tarjeta PCI tipo Matrox Millennium:

¹"Gris" indica aquí que se trata de teclas del bloque numérico, ya que éstas se resaltan a veces en color gris.

```

Section "Device"
    BoardName      "MGA2064W"
    BusID          "0:19:0"
    Driver         "mga"
    Identifier     "Device[0]"
    VendorName     "Matrox"
    Option         "sw_cursor"
EndSection

```

La apariencia de la sección **Device** debería ser semejante a la que se refleja arriba, en caso de usar **SoX2** para la configuración. **SoX2** determina **Driver** y **BusID** que dependen del hardware usado por la máquina a configurar. **BusID** determina la posición que ocupa la tarjeta gráfica en el bus PCI o AGP y es equivalente al número que **lspci** indica. ¡Hay que tener en cuenta que el servidor **X** usa valores decimales mientras que los de **lspci** con hexadecimales!

El parámetro **Driver** determina el driver para la tarjeta gráfica que para el caso de la Matrox Millennium es **mga**. El servidor **X** busca el driver en el subdirectorio **drivers** de la rama **ModulePath** definido en el apartado **Files**. La rama completa para una instalación estándar es **/usr/X11R6/lib/modules/drivers**. El nombre completo del driver se obtiene añadiendo **_drv.o** al identificador corto, lo que resulta en nuestro ejemplo en **mga_drv.o**.

Existen opciones adicionales para activar ciertas características del servidor **X** y de su driver. En este caso se ha usado como ejemplo la opción **sw_cursor** que desactiva el cursor hecho por hardware para emularlo mediante software. Según el driver usado, hay diferentes opciones que se explican junto con los drivers en el directorio **/usr/X11R6/lib/X11/doc**. Hay opciones generales en la página del manual de **XF86Config** (man **XF86Config**) y la página del manual de **XFree86** (man **XFree86**).

Secciones Monitor y Modes

Las secciones de **Monitor** y de **Modes**, así como las de **Device**, describen un monitor por cada sección y puede haber una cantidad infinita de estas secciones en el fichero de configuración **/etc/X11/XF86Config**. En la sección de **ServerLayout** se determina qué sección de monitor vale a efectos de la configuración.

Sólo usuarios muy experimentados deberían generar o ajustar una sección de **Monitor** (y sobre todo la de **Modes**) al igual que una sección de tarjeta gráfica. Una parte fundamental de la sección **Modes** son los "Modelines" que indican las sincronizaciones (ingl. *timings*) horizontales y verticales para cada resolución. La sección **Monitor** contiene las características del monitor y entre ellas sobre todo las frecuencias de refresco máximas.

Aviso

¡Sin un buen conocimiento de la función de monitor y de tarjeta gráfica no se debería cambiar ningún valor de los Modelines, ya que esto podría provocar la destrucción del monitor!

Aviso

Si realmente se atreve a hacer sus propias configuraciones de monitor, debería leer antes la documentación en `/usr/X11/lib/X11/doc`. Se recomienda especialmente la lectura de `?` que explica detalladamente la función del hardware y la definición de los Modelines.

Por fortuna hoy en día, casi nunca hace falta generar Modelines o definiciones de monitores "a mano". Usando un monitor de multifrecuencia moderno, SxX2 puede leer vía DDC los rangos de frecuencia admitidas y las resoluciones óptimas, directamente desde el monitor. Si esto no fuera posible, siempre se puede recurrir a uno de los modos VESA del servidor X que funcionan prácticamente con todas las combinaciones posibles de monitor y de tarjeta gráfica.

Incorporar fuentes (TrueType) adicionales

Junto con la instalación normal de un servidor X11R6, se instala una cierta cantidad de fuentes que se encuentran dentro del directorio `/usr/X11R6/lib/X11/fonts` ordenadas de forma lógica en sub-directorios. El servidor X solo tiene en cuenta un sub-directorio si se cumple que:

- está apuntado como `FontPath` en el apartado `Files` del fichero `/etc/X11/XF86Config`.
- contiene un fichero `fonts.dir` válido.
- no fue dado de baja durante la ejecución del servidor X mediante el comando `xset -fp`.
- fue dado de alta durante la ejecución del servidor X mediante el comando `xset +fp`.

Aparte del formato propio `Type1` (un formato de PostScript) y de `pcf` para fuentes de bitmap escalables, con la versión 4.0 XFree86 maneja también el nuevo formato `ttf` (ingl. *true type font*). Estas fuentes se soportan, como en el apartado [La versión 4.x de XFree86](#) en la página 101, mediante módulos que carga el servidor X. Para usar las fuentes TrueType ya no hacen falta muchos preparativos.

Aparte de la buena escalabilidad, la gran ventaja de la mayoría de las fuentes TrueType es el gran abanico de caracteres incluidos que supera ampliamente los normales 255 caracteres del juego de caracteres "iso-8859-1" para Europa occidental. En consecuencia se puede trabajar sin problemas en cirílico, griego o en otros idiomas de Europa oriental. Con software adicional incluso funcionan las lenguas asiáticas.

La presente explicación contempla sobre todo el uso de juegos de caracteres de 8 bits. Sin embargo también queda la posibilidad de introducir caracteres de un idioma asiático (japonés, chino) usando unos editores especiales que forman parte de SuSE Linux.

Los juegos de caracteres de 8 bits están formados por 256 caracteres, ampliando así el juego ASCII que se restringe a los primeros 128 caracteres. De esta forma cada letra ocupa 8 bits en la memoria. Los 128 caracteres adicionales del juego ampliado no son suficiente para representar todos los caracteres especiales p. ej. de todos los idiomas europeos. Por tanto los idiomas están agrupados y se representan con una determinada abreviatura que corresponde a la norma aplicada p. ej. "iso-8859-x". 'x' es una cifra entre 1 y 15. La asignación exacta de los caracteres p. ej. en el juego de iso-8859-1 respectivamente iso-8859-15 se puede encontrar en la página del manual de iso-8859-1 (man iso-8859-1) respectivamente página del manual de iso-8859-15 (man iso-8859-15).

Algunos códigos de los juegos de caracteres se encuentran en la tabla 5.2, otros se encuentran en la página del manual mencionada.

Juego de caracteres	Región, idiomas incluidos
iso-8859-1	Idiomas de Europa occidental: español, alemán, francés, sueco, finlandés, danés, etc.; para finlandés y francés ahora es más adecuado iso-8859-15
iso-8859-2	Centro-Europa y del este: húngaro, checo, rumano, polaco, alemán, etc.
iso-8859-5	Caracteres del cirílico para el ruso
iso-8859-7	Caracteres para el griego
iso-8859-15	Igual a iso-8859-1, pero con caracteres para el turco y el carácter para el Euro.

Cuadro 5.2: Códigos de juegos de caracteres importantes

El usuario tiene que seleccionar la codificación de acuerdo al idioma usado. Transfiriendo texto entre diferentes ordenadores, éste se ha de transferir jun-

to con su codificación. La ventaja de este sistema es la sencilla implementación del soporte de los caracteres especiales. Una vez seleccionada la codificación correcta, todos los programas (o casi todos) pueden visualizar estos caracteres, ya que la gran mayoría trabaja con un valor de 8 bits (un byte) para cada letra. Por otra parte los caracteres especiales se muestran mal, cuando la codificación seleccionada no es la adecuada. Para la mayoría de los programas del sistema X Window y del entorno KDE se puede seleccionar la codificación del juego de caracteres; esto se realiza normalmente junto con la configuración del tipo de caracteres (p. ej. Helvética, Courier, Times, etc). Los programas del entorno gráfico denominan la codificación normalmente como **Encoding**.

La desventaja de esta solución es la imposibilidad de representar en pantalla ciertas combinaciones de idiomas. Sin tomar medidas adicionales no es posible p. ej. mencionar nombre propios en cirílico dentro de un texto en castellano.

La solución a este dilema pasa por Unicode que codifica los caracteres mediante 2 o más bytes, por lo que se puede trabajar con muchos más caracteres al mismo tiempo. Sólo gracias a Unicode es posible trabajar con idiomas asiáticos que tienen muchos más de 127 caracteres como p. ej. chino, japonés o coreano. La desventaja es que la mayor parte del software no está preparada para procesar estas letras y sólo mediante software especial es posible leer o escribir letras en Unicode. Hay información adicional sobre el uso de Unicode en Linux en <http://www.unicode.org>. Es de suponer que con el tiempo el soporte de Unicode vaya creciendo; SuSE Linux ya incorpora el programa `yudit` para introducir letras en Unicode. Este programa se encuentra en el paquete `yudit`, serie `xap` y, una vez hecha la instalación, en el menú de SuSE bajo **Business/Office y Editores**.

Después de esta introducción general, se presenta una descripción paso a paso de la instalación de fuentes adicionales, tomando como ejemplo fuentes TrueType.

Averigüe dónde se encuentran las fuentes que quiere instalar en el sistema X Window. Si su sistema dispone de fuentes TrueType con licencia, puede usar éstas mismas. Para ello monte simplemente la partición que contiene estas fuentes y cambie al directorio de las fuentes. SuSE Linux ya ha preparado un directorio denominado `/usr/X11R6/lib/X11/fonts/truetype`, donde puede copiar las fuentes en cuestión.

```
tierra:/root # cd /usr/X11R6/lib/X11/fonts/truetype
```

Ahora cree enlaces simbólicos a los ficheros `ttf`. Sustituya `/ruta/a/las/fuentes` por la ruta bajo la que se encuentran estas fuentes. A continuación ejecute `SuSEconfig`, que creará las entradas necesarias en el fichero `fonts.dir`.

```
tierra:/usr/X11R6/lib/X11/fonts/truetype #  
ln -s </ruta/a/las/fuentes>/*.ttf .  
tierra:/usr/X11R6/lib/X11/fonts/truetype #  
SuSEconfig -module fonts
```

Para dar de alta las fuentes cuando el servidor X ya está en ejecución, use el comando:

```
tierra:~ # xset fp rehash
```

Truco

El comando `xset` accede al servidor X mediante el protocolo X, por lo que debe tener derechos de acceso al servidor en ejecución. Este se consigue p. ej., cuando `tux` es idéntico al usuario que ha iniciado el servidor X. Hay más información en la página del manual de `xauth` (`man xauth`).

Truco

Puede comprobar si las fuentes han sido configuradas correctamente con el programa `xlsfonts`. Si está todo correctamente configurado, éstas aparecen en una lista que debe incluir la fuente TrueType recién instalada. Otra posibilidad es usar el gestor de fuentes de KDE que muestra las fuentes instaladas junto con un ejemplo de texto. Se arranca desde el centro de control de KDE.

```
tierra:~ # xlsfonts
```

Todos los programas del sistema X Window pueden usar ahora las fuentes que se hayan configurado de esta forma.

Configuración de OpenGL/3D

OpenGL es la interfaz de 3D para Linux. Direct3D de Microsoft no está disponible para Linux.

Hardware Soportado

SuSE Linux incluye varios controladores OpenGL para el siguiente hardware 3D. La Tabla 5.3 en la página siguiente le proporciona una visión general.

Controlador OpenGL	Hardware soportado
nVidia-GLX / XFree86 4.x	nVidia Chips: todos aparte de 128(ZX)
DRI / XFree86 4.x	3Dfx Voodoo Banshee 3Dfx Voodoo-3/4/5 Intel i810/i815/i830M Intel 845G/852GM/855GM/865G Matrox G200/G400/G450/G550 ATI Rage 128(Pro)/Radeon

Cuadro 5.3: Hardware 3D soportado

Si está realizando una nueva instalación con YaST, puede activar el soporte 3D durante la instalación siempre y cuando YaST detecte dicho soporte. Los chips gráficos nVidia son la única excepción; en este caso, el controlador incluido "Dummy" deberá ser reemplazado por el controlador nVidia oficial. Utilice YOU (la actualización en línea de YaST) para actualizar los paquetes `NVIDIA_GLX` y `NVIDIA_kernel`. Si no es posible una actualización con YOU, deberá bajarse los paquetes RPM `NVIDIA_GLX` y `NVIDIA_kernel` del servidor web de nVidia (<http://www.nvidia.com>) e instalarlos. Debido a las cláusulas de la licencia, sólo podemos ofrecerle los controladores nVidia "Dummy".

Si va a realizar una actualización, el soporte de hardware 3D tendrá que configurarse de manera diferente. El método depende del controlador OpenGL que esté utilizando y se describe con más detalle en la siguiente sección.

Controladores OpenGL

nVidia-GLX y DRI

Este controlador OpenGL puede instalarse muy fácilmente utilizando SaX2. Si dispone de una tarjeta nVidia, SaX2 necesitará reemplazar el controlador de SuSE "Dummy" por los controladores oficiales de nVidia mediante una actualización en línea. El comando `3Ddiag` le permite comprobar si el nVidia-GLX o DRI están configurados correctamente.

Por razones de seguridad, sólo los usuarios que pertenecen al grupo `video` pueden tener acceso al hardware 3D. Compruebe que todos los usuarios que trabajan localmente en la máquina pertenecen a ese grupo. De no ser así, cuando intente ejecutar aplicaciones OpenGL se ejecutará el *Software Rendering Fallback* del controlador OpenGL. Utilice el comando `id` para comprobar si el usuario actual pertenece al grupo `video`. Si éste no es el caso, utilice YaST para añadirlo al grupo.

Herramienta de diagnóstico 3Ddiag

Puede verificar la configuración 3D en SuSE Linux con la herramienta de diagnóstico 3Ddiag incluida en el sistema. Se debe ejecutar este comando desde una terminal de línea de comandos.

La aplicación examinará, por ejemplo, la configuración de XFree86 para verificar que los paquetes de soporte de 3D están instalados y las librerías OpenGL están siendo utilizadas con la extensión GLX. Siga las instrucciones de 3Ddiag si aparecen mensajes de "failed". Si todo ha ido a la perfección, verá en la pantalla el mensaje "done".

3Ddiag -h proporciona información sobre las opciones admitidas por 3Ddiag.

Aplicaciones de prueba OpenGL

Para probar OpenGL puede utilizar juegos tales como **tuxracer** y **armagetron** (del paquete del mismo nombre) así como **glxgears**. Si el soporte 3D ha sido activado, estos juegos funcionarán correctamente en ordenadores medianamente actuales. Sin embargo, sin soporte 3D no será posible ejecutarlos o sólo con graves efectos de distorsión. La salida del comando **glxinfo** le informará de si el soporte 3D está activado. La variable "direct rendering" ha de tener el valor "Yes".

Resolución de problemas

Si los resultados de la prueba de 3D de OpenGL han sido negativos (los juegos no se han visualizado adecuadamente), utilice 3Ddiag para asegurarse de que no existen errores en la configuración (mensajes de "failed"). Si la corrección de estos no ayuda o no han aparecido mensajes de error, mire los archivos log de XFree86. A menudo, encontrará aquí la línea "DRI is disabled" en los archivos **XFree86 4.x /var/log/XFree86.0.log**. Se puede descubrir la causa exacta examinando con detalle los archivos log, lo que quizá sea demasiado complicado para un usuario no experimentado.

En estos casos, lo normal es que no exista ningún error en la configuración, puesto que ya habría sido detectado por 3Ddiag. Por lo tanto sólo queda el Software Rendering Fallback del controlador DRI, el cual no ofrece soporte de hardware 3D. Prescinda también del soporte 3D en caso de fallos de representación en OpenGL o problemas generales de estabilidad. Puede desactivar el soporte 3D con **SaX2**.

Soporte de instalación

Aparte de Software Rendering Fallback del controlador DRI, todos los controladores de Linux están en fase de desarrollo y por tanto se consideran en pruebas. Los controladores se incluyen en la distribución debido a la alta demanda de aceleración de hardware 3D en Linux. Considerando el estado experimental de los controladores de OpenGL, no podemos ofrecer un soporte de instalación para configurar la aceleración de hardware 3D o proporcionar ningún otro tipo de ayuda. La configuración básica de la interfaz gráfica X11 no incluye la configuración de la aceleración de hardware 3D.

No obstante, esperamos que este capítulo responda a muchas preguntas relacionadas con este tema. En caso de problemas con el soporte de hardware 3D le recomendamos en última instancia prescindir de este soporte.

Documentación on line adicional

- nVidia-GLX: `/usr/share/doc/packages/nv_glx/`,
`/usr/src/kernel-modules/nv_glx/README` (paquetes
`NVIDIA_GLX` y `NVIDIA_kernel` del servidor de nVidia)
- DRI: `/usr/X11R6/lib/X11/doc/README.DRI` (paquete `XFree86`)
- Mesa general: `/usr/share/doc/packages/mesa/` (paquete `mesa`)

Funcionamiento de la impresora

El presente capítulo le ofrece información detallada sobre el funcionamiento de la impresora. Los ejemplos incluidos posibilitan una comprensión más profunda del entorno de impresión, lo que le será de gran ayuda para encontrar la solución correcta a distintos problemas y evitar diagnósticos e intentos de resolución incorrectos.

Fundamentos del proceso de impresión	126
Requisitos para imprimir	129
Configuración de impresoras con YaST	134
Configuración para aplicaciones	140
Configuración manual de puertos locales	140
Configuración manual de LPRng/lpdfilter	145
El spooler de impresión LPRng	146
Herramientas de línea de comandos para LPRng	147
El filtro de impresión del sistema LPRng/lpdfilter	152
El sistema de impresión CUPS	161
Imprimir desde aplicaciones	168
Herramientas de línea de comandos para el sistema de impresión CUPS	169
Acerca de Ghostscript	173
Acerca de a2ps	177
Reformatear PostScript con psutils	178
Codificación de texto ASCII	181
Impresión en redes TCP/IP	183

Fundamentos del proceso de impresión

En Linux las impresoras funcionan mediante *colas de impresión*. Los datos a imprimir se envían a una cola de impresión donde se almacenan temporalmente hasta que son reenviados sucesivamente a la impresora a través del spooler de impresión.

La mayoría de las veces los datos a imprimir no se encuentran en la forma adecuada para ser enviados directamente a la impresora. Así por ejemplo, un gráfico debe ser convertido previamente a otro formato que la impresora pueda reproducir directamente. Esta conversión al *lenguaje de impresión* se realiza mediante un *filtro de impresión* que es activado por el spooler para convertir los datos de impresión a un formato que la impresora pueda imprimir directamente.

Ejemplos de lenguajes de impresión estándar

Texto ASCII La mayoría de las impresoras pueden al menos imprimir directamente texto ASCII. Las pocas excepciones que existen entienden alguno de los siguientes lenguajes de impresión.

PostScript *PostScript* es el lenguaje de impresión estándar utilizado para tareas de impresión en Unix/Linux, las cuales pueden ser imprimidas por las impresoras PostScript directamente. Este tipo de impresoras es relativamente caro, ya que PostScript es un complejo y poderoso lenguaje que exige un alto rendimiento por parte del ordenador a la hora de imprimir. Además la licencia provoca costes adicionales.

PCL3, PCL4, PCL5e, PCL6, ESC/P, ESC/P2 y ESC/P Raster Si no hay una impresora PostScript conectada, el filtro de impresión utiliza el programa Ghostscript para convertir los datos en uno de los otros lenguajes de impresión estándar. Para ello se debe utilizar un controlador Ghostscript adecuado para el modelo de impresora de que se trate, con el fin de poder tener en cuenta las particularidades específicas de cada modelo (p. ej. opciones de color).

Desarrollo de un trabajo de impresión

1. El usuario o un programa de aplicación lanza un trabajo de impresión.

2. Los datos a imprimir se guardan en la cola de impresión, desde donde son reenviados por el spooler de impresión al filtro de impresión correspondiente.
3. El filtro de impresión realiza por lo general lo siguiente:
 - a) Se identifica el tipo de datos que se va a imprimir.
 - b) Si no se trata de datos PostScript, se transforman en datos de este lenguaje estándar. En especial se convierte el texto ASCII en lenguaje PostScript.
 - c) En caso necesario, los datos PostScript se convierten a otro lenguaje que la impresora pueda entender.
 - Si se trata de una impresora PostScript, se envían los datos PostScript directamente a la impresora.
 - Si no se trata de una impresora PostScript, el programa Ghostscript emplea un controlador que se acomoda al lenguaje de impresión del modelo de impresora utilizado. Este controlador transforma los datos PostScript en datos escritos en el lenguaje de impresión correspondiente, que luego serán enviados a la impresora.
4. Una vez que el trabajo de impresión ha sido enviado en su totalidad a la impresora, el spooler de impresión lo borra de la cola de impresión.

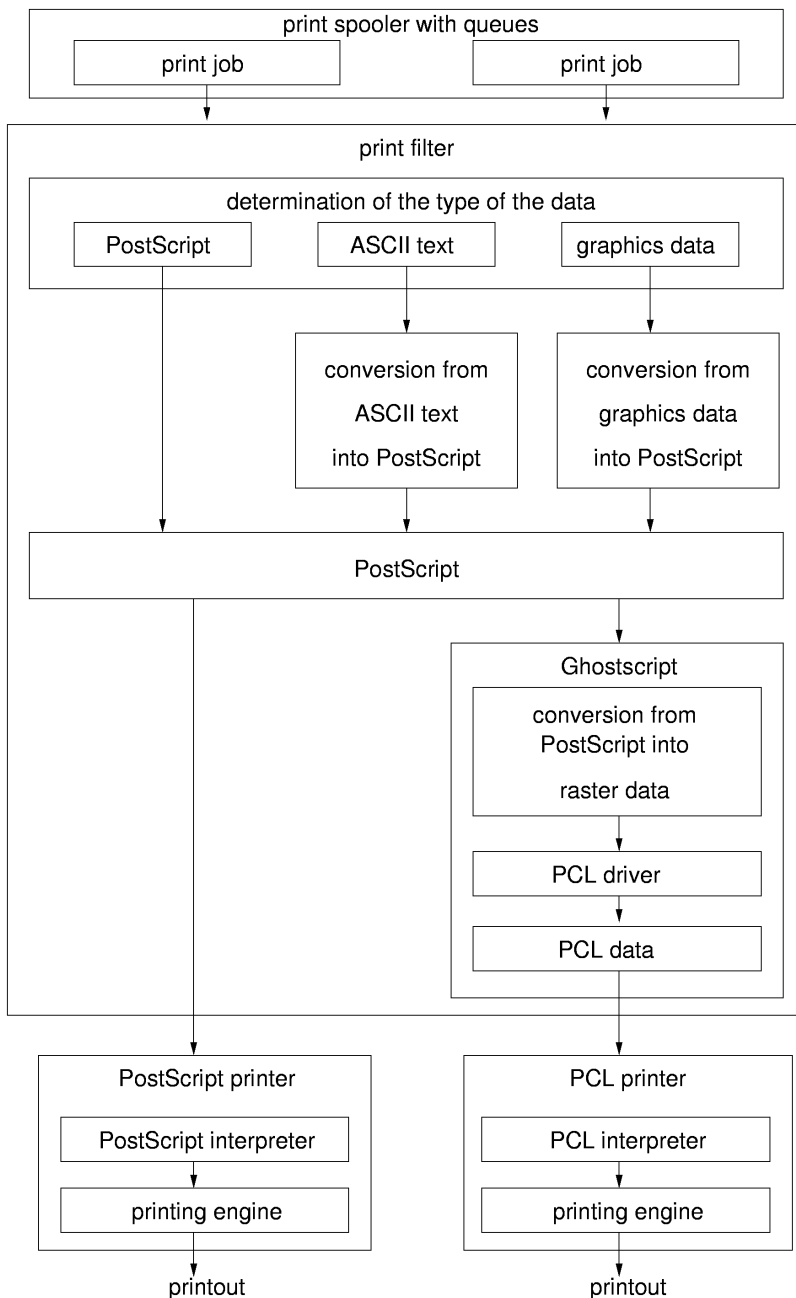


Figura 6.1: Resumen del proceso de impresión

Distintos sistemas de impresión

SuSE Linux soporta dos tipos de sistemas de impresión:

LPRng/lpdfilter Este es un sistema tradicional compuesto por el spooler de impresión LPRng y el filtro de impresión lpdfilter. En sistemas tradicionales, el administrador del sistema establece toda la configuración de una cola de impresión y el usuario sólo puede escoger entre distintas colas. Para elegir una determinada configuración, deben fijarse varias colas de impresión con distintas configuraciones para la misma impresora. En impresoras de blanco y negro (p. ej. la mayoría de las impresoras láser) basta con una configuración estándar, pero con las modernas impresoras a chorro de tinta en color es necesario realizar distintas configuraciones para imprimir en blanco y negro, en color, en color a gran resolución o con calidad fotográfica. Mediante este tipo de configuraciones se garantiza automáticamente que sólo se utilizarán aquellas realizadas por el administrador del sistema. Por otro lado, ya que el usuario no puede realizar configuraciones individuales, el administrador del sistema debe configurar muchas colas de impresión para poder aprovechar todas las posibilidades que ofrecen las impresoras actuales y ponerlas a disposición de los usuarios.

CUPS Con el sistema CUPS el usuario tiene la posibilidad de definir para cada impresión propiedades diferentes ya que aquí el administrador del sistema no determina la configuración total de una cola de impresión. Las distintas posibilidades de configuración se encuentran en un archivo PPD (ingl. *PostScript Printer Description*) para cada cola de impresión. Este archivo se le presenta al usuario en una ventana de diálogo. Normalmente el archivo PPD contiene todas las posibilidades que ofrece la impresora. No obstante, el administrador del sistema puede modificar este archivo y limitar esas posibilidades.

Debido a que pueden originarse conflictos entre los dos sistemas, normalmente no es posible tener instalados ambos sistemas de impresión *simultáneamente* en el sistema. YaST permite cambiar de un sistema a otro – ver *Manual de Usuario*, sección *YaST — Configuración, Impresoras*.

Requisitos para imprimir

Requisitos generales

- SuSE Linux debe soportar la impresora; véase las siguientes fuentes de información:

Base de datos de impresoras de SuSE <http://cdb.suse.de> o bien <http://hardwaredb.suse.de/>

Base de datos de impresoras de Linuxprinting.org <http://www.linuxprinting.org/> ("The Database" <http://www.linuxprinting.org/database.html> o bien la lista http://www.linuxprinting.org/prINTER_list.cgi)

Ghostscript <http://www.cs.wisc.edu/~ghost/>

Controladores Ghostscript en SuSE Linux <file:/usr/share/doc/packages/ghostscript/catalog.devices> Aquí puede encontrar una lista de los controladores Ghostscript incluidos en la versión actual de SuSE Linux. Esto es muy importante ya que a veces en WWW se menciona un controlador Ghostscript que no está incluido en SuSE Linux. Por motivos de licencias, los controladores contenidos en SuSE Linux son "Ghostscript GNU". Pero por lo general, siempre habrá un controlador Ghostscript GNU que funcione con la impresora.

- Debe ser posible comunicarse con la impresora; véase la sección *Configuración manual de puertos locales* en la página 140 o bien *Configuración manual* en la página 137.
- Debe utilizar un kernel original de SuSE sacado de los CD-ROMs, en especial kernels que *no* haya compilado Vd. mismo. Si se producen problemas, instale un kernel original de SuSE y arranque de nuevo.
- Le recomendamos que realice la instalación del 'Sistema estándar' con YaST para que todos los paquetes necesarios estén disponibles. Si en la instalación del sistema estándar no ha cambiado la selección predeterminada de paquetes, está todo en regla. En caso contrario, instale al menos el 'Sistema estándar'. Los 'Sistemas mínimos' no bastan para imprimir.

Determinar el controlador de impresión correcto

No es necesario ningún controlador de impresión especial para una impresora PostScript. Véase la sección *Desarrollo de un trabajo de impresión* en la página 126. Para impresoras que no soporten PostScript, un controlador Ghostscript se encargará de crear los datos específicos para esa impresora. Por tanto los controladores Ghostscript son el punto decisivo en el que se especifica el tipo de impresión en aquellas impresoras que no soporten PostScript. Los datos impresos son determinados por las configuraciones específicas del controlador

Ghostscript seleccionado. Las listas del apartado [Requisitos generales](#) en la página 129 indican también los controladores de Ghostscript específicos para determinados modelos de impresoras

Si no encuentra ningún controlador Ghostscript para su impresora, pregúntele al fabricante de la misma qué lenguaje de impresión entiende el modelo de impresora. Algunos fabricantes proporcionan incluso controladores Ghostscript especiales para sus impresoras. Aunque el fabricante no pueda ofrecerle ninguna información sobre el funcionamiento de la impresora en Linux, sí podrá facilitarle otros datos que le ayudarán a encontrar el controlador adecuado:

- Averigüe si su impresora es compatible con un modelo que funcione con Linux y utilice en ese caso el controlador de Ghostscript del modelo compatible. Ser compatible con Linux significa que su impresora puede imprimir correctamente la misma secuencia binaria que el modelo compatible – ambas impresoras “entienden” directamente el mismo lenguaje de impresión, sin necesidad de usar un controlador o un programa de emulación (para otro sistema operativo).

Las impresoras con nombres o descripciones parecidos no son necesariamente compatibles, ya que no siempre entienden el mismo lenguaje de impresión.

- La forma más segura de averiguar el lenguaje de la impresora es consultar al fabricante. Esta información se encuentra generalmente también en el manual que acompaña a la impresora.

PCL5e o PCL6 Las impresoras que entienden directamente *PCL5e* o *PCL6* deberían funcionar con un controlador Ghostscript ljet4 con hasta 600x600 dpi. PCL5e también se conoce a menudo como PCL5.

PCL4 o PCL5 Las impresoras que entienden directamente *PCL4* o *PCL5* deberían funcionar con un controlador Ghostscript laserjet, ljetplus, ljet2p o ljet3, pero están limitadas a 300x300 dpi.

PCL3 Las impresoras que entienden *PCL3* directamente deberían funcionar con un controlador Ghostscript deskjet, hpdj, pcl3, cdjmono, cdj500 o cdj550.

ESC/P2, ESC/P o ESC/P Raster Las impresoras que entienden directamente *ESC/P2*, *ESC/P* o *ESC/P Raster* deberían funcionar con un controlador Ghostscript stcolor o con uniprint además de utilizar un archivo de parámetros .upp adecuado (p.ej. stcany .upp).

La problemática de las impresoras GDI

Puesto que normalmente los fabricantes de hardware no desarrollan controladores de impresoras para Linux, se recomienda que la impresora a instalar entienda uno de los lenguajes de impresión más conocidos como *PostScript*, *PCL* o *ESC/P*. Las impresoras normales entienden al menos uno de estos lenguajes de impresión, pero hay fabricantes que desarrollan impresoras con las que sólo es posible comunicarse con la versión específica del sistema operativo para la que el fabricante proporciona el controlador; a estas impresoras se las denomina *impresoras GDI*. Puesto que tales impresoras no siguen normas estándar, a menudo se producen dificultades cuando se las quiere utilizar con Linux.

GDI es una interfaz desarrollada por Microsoft para la representación gráfica. El problema no es la interfaz, sino que *sólo* se puede acceder a la impresora *GDI* utilizando el lenguaje de impresión propietario del correspondiente modelo de impresora. En realidad sería más correcto decir: "la impresora a la que *sólo* es posible hablar utilizando un lenguaje de impresión propietario".

Pero hay impresoras que, además del modo *GDI*, entienden un lenguaje de programación estándar, para lo cual hay que configurar o cambiar el modo de la impresora convenientemente. Si junto a Linux utiliza otro sistema operativo, puede que el controlador de impresión del otro sistema operativo haya puesto la impresora en modo *GDI*, con lo que ésta no funcionaría después con Linux. O vuelve a poner la impresora en el otro sistema operativo en modo estándar, o la utiliza solamente en modo estándar también en el otro sistema operativo, aunque las posibilidades de impresión sean entonces más reducidas (p. ej. una menor resolución).

De un tipo especial son las impresoras que sólo entienden partes rudimentarias de un lenguaje de impresión estándar — sólo los comandos necesarios para la impresión de datos gráficos. A veces tales impresoras pueden utilizarse normalmente, ya que por lo general los controladores Ghostscript sólo utilizan los comandos para la impresión de datos gráficos. Puede ocurrir entonces que no se pueda enviar texto ASCII directamente a la impresora, pero Ghostscript suele estar siempre disponible. Especialmente problemáticas son las impresoras que deben ser adaptadas mediante secuencias especiales. Aquí no se puede utilizar ningún controlador Ghostscript normal, sino que se necesita un controlador especial que realice esta adaptación.

Existen controladores específicos del fabricante para algunas impresoras *GDI*. El inconveniente de estos controladores en Linux *para impresoras GDI* consiste en que no se puede garantizar que funcionen con las distintas versiones (futuras) de Linux.

Las impresoras, que entienden un lenguaje de impresión estándar público no dependen ni de un sistema operativo determinado ni de una versión especial de

un sistema operativo, y los controladores Linux específicos del fabricante para tales impresoras a menudo ofrecen los mejores resultados de impresión.

SuSE Linux soporta las siguientes impresoras GDI a través de la configuración de impresoras con YqST, pero puesto que estas impresoras siempre dan problemas, puede que algún modelo no funcione o que existan grandes restricciones como p. ej. que sólo se pueda imprimir en blanco y negro y con baja resolución. Tenga en cuenta que no podemos garantizar la fiabilidad de esta información puesto que no probamos los controladores de impresoras GDI.

- Brother HL 720/730/820/1020/1040, MFC 4650/6550MC/9050 y modelos compatibles.
- HP DeskJet 710/712/720/722/820/1000 y modelos compatibles.
- Lexmark 1000/1020/1100/2030/2050/2070/3200/5000/5700/7000/7200, Z11/42/43/51/52 y modelos compatibles.
- Oki Okipage 4w/4w+/6w/8w/8wLite/8z/400w y modelos compatibles.
- Samsung ML-200/210/1000/1010/1020/1200/1210/1220/4500/5080/6040 y modelos compatibles.

Por lo que sabemos, la siguientes impresoras GDI *no* están soportadas por SuSE Linux, pero seguramente esta lista no sea completa:

- Brother DCP-1000, MP-21C, WL-660
- Canon BJC 5000/5100/8000/8500, LBP 460/600/660/800, MultiPASS L6000
- Epson AcuLaser C1000, EPL 5500W/5700L/5800L
- HP LaserJet 1000/3100/3150
- Lexmark Z12/22/23/31/32/33/82, Winwriter 100/150c/200
- Minolta PagePro 6L/1100L/18L, Color PagePro L, Magicolor 6100DeskLaser, Magicolor 2 DeskLaser Plus/Duplex
- Nec SuperScript 610plus/660/660plus
- Oki Okijet 2010
- Samsung ML 85G/5050G, QL 85G
- Sharp AJ 2100, AL 1000/800/840/F880/121

Configuración de impresoras con YaST

Colas de impresión y configuración

Normalmente se necesitan varias colas de impresión por los siguientes motivos:

- Se debe acceder a distintas impresoras a través de distintas colas de impresión.
- En cada cola de impresión se puede configurar el filtro de impresión individualmente. Así pues, se pueden utilizar distintas colas de impresión para la misma impresora para poner distintas configuraciones a disposición de los usuarios. En CUPS no es necesario, ya que el propio usuario puede definir la configuración adecuada. Véase a este efecto la sección *Distintos sistemas de impresión* en la página 129.

Para imprimir en blanco y negro (p. ej. la mayoría de las impresoras láser) basta una sola configuración estándar, pero para las impresoras a chorro de tinta en color se necesita al menos dos configuraciones — o sea, dos colas de impresión.

- Una configuración estándar con la que la impresora puede imprimir en blanco y negro rápidamente y con un bajo coste.
- Una configuración “en color” o, lo que es lo mismo, una cola de impresión para impresión en color.

Fundamentos de la configuración de impresoras con YaST

La configuración de impresoras de YaST no sólo se puede iniciar mediante menús, sino también como usuario `root` directamente desde la línea de comandos con el comando `yast2 printer .nodetection`. Con `yast2 printer .nodetection` se puede evitar la detección automática de impresoras. Véase la sección *Puertos paralelos* en la página 140.

No todas las impresoras pueden configurarse para ambos sistemas de impresión. Algunas configuraciones son soportadas o sólo por CUPS o sólo por LPRng/lpdfilter. La configuración de impresoras de YaST se lo indica en caso necesario.

Con la configuración de impresoras de YaST se puede cambiar entre CUPS y LPRng/lpdfilter con facilidad a través del botón ‘Avanzado’.

Con YaST se puede cambiar entre los siguientes sistemas de impresión:

CUPS como servidor (configuración por defecto en la instalación estándar)

Si una impresora está conectada localmente, CUPS debe funcionar como servidor. En caso de no configurar ninguna cola local con YdST, el daemon de CUPS cupsd no será iniciado automáticamente. Si a pesar de todo quiere que cupsd funcione, ha de activar el servicio 'cups' (normalmente para los niveles de ejecución 3 y 5) – véase la sección [Configuración rápida de un cliente](#) en la página 184. Se deben instalar los siguientes paquetes para este sistema de impresión:

- cups-libs
- cups-client
- cups
- footmatic-filters
- cups-drivers
- cups-drivers-stp

CUPS exclusivamente como cliente Si hay un servidor de red CUPS en la red local (véase la sección [Aclaración de términos](#) en la página 183) y el usuario sólo quiere imprimir a través de esa cola de impresión, basta con que CUPS funcione exclusivamente como cliente – véase la sección [Configuración rápida de un cliente](#) en la página 184. Son necesarios los siguientes paquetes:

- cups-libs
- cups-client

LPRng Seleccione esta opción si se debe utilizar el sistema de impresión LPRng/lpdfilter o si la red local sólo dispone de un servidor de red LPD (véase sección [Aclaración de términos](#) en la página 183), y el usuario quiere imprimir a través de esta cola de impresión – véase la sección [Configuración rápida de un cliente](#) en la página 184. Los paquetes a instalar son los siguientes:

- lprng
- lpdfilter
- footmatic-filters
- cups-drivers

El paquete cups-client y el paquete lprng se excluyen mutuamente y por tanto no pueden ser instalados a la vez. El paquete cups-libs siempre debe

estar instalado, ya que algunos programas (p. ej. Ghostscript, KDE, Samba, Wine y la configuración de impresoras de YaST necesitan las bibliotecas CUPS. Para disponer de un sistema de impresión completo normalmente se necesitan también algunos paquetes adicionales, instalados automáticamente con el ‘Sistema estándar’:

- `ghostscript-library`
- `ghostscript-fonts-std`
- `ghostscript-x11`
- `libgimprint`

La configuración de impresoras de YaST muestra las configuraciones que se pueden realizar sin que ocurra ningún error.

Puesto que la configuración se crea de hecho al terminar la configuración de YaST, se debe arrancar de nuevo la configuración de YaST para comprobar.

La configuración de impresoras de YaST distingue entre colas de impresión definidas con YaST (colas de impresión YaST) y aquellas que no han sido definidas con YaST (colas de impresión sin YaST), las cuales YaST no modifica. El conflicto llega cuando el nombre es idéntico. Al editar una cola de impresión se puede elegir si YaST ha de ocuparse de su configuración o no. Al convertir una cola YaST en una cola sin YaST es posible realizar modificaciones propias sin que YaST sobrescriba los cambios efectuados. El proceso inverso también es posible (convertir una cola sin YaST en una cola YaST). En este caso la configuración de la cola podrá sobrescribirse con la configuración de YaST.

Configuración automática

En función del hardware que YaST detecte automáticamente y de la cantidad de información sobre el correspondiente modelo de impresora que se encuentre en la base de datos de impresoras de YaST, éste podrá proporcionar los datos necesarios automáticamente u ofrecer una preselección adecuada. En caso contrario, el usuario debe dar la información necesaria en los cuadros de diálogo. Con YaST se puede configurar la impresora automáticamente si se cumplen los siguientes requisitos:

- La configuración automática del puerto paralelo o USB funciona gracias al reconocimiento automático de hardware y la impresora conectada es detectada automáticamente.

- La base de datos de impresoras contiene la identificación del modelo de impresora que YaST obtiene durante el reconocimiento automático. La información detectada puede variar con respecto a la denominación de modelo y es posible que el modelo sólo pueda ser seleccionado manualmente.

Es esencial comprobar cada configuración mediante la página de prueba de YaST, ya que a menudo las configuraciones se introducen en la base de datos de impresoras sin un soporte explícito del fabricante de la impresora, y por tanto no se puede garantizar el funcionamiento de todas las entradas de la base de datos.

Además la página de prueba de YaST ofrece mucha información importante acerca de la configuración en cuestión.

Configuración manual

Se precisa de una configuración manual cuando alguno de los requisitos para el funcionamiento de la configuración automática no se cumple o cuando se trata de realizar una configuración personalizada. Es necesario configurar los siguientes valores:

Conexión de hardware (puerto)

- En el caso de que YaST haya detectado el modelo de impresora automáticamente, se supone que el puerto de conexión a la impresora funciona correctamente y por lo tanto no es necesario configurarlo.
- Pero si YaST no detecta el modelo de impresora automáticamente, esto indica que el puerto de conexión a la impresora debe ser configurado manualmente. En una configuración manual se debe escoger el puerto apropiado. `/dev/lp0` es el primer puerto paralelo. `/dev/usb/lp0` es el puerto para una impresora USB. En este caso se debe realizar sin falta la correspondiente prueba en YaST para comprobar si es posible acceder a la impresora a través del puerto elegido.

El método más seguro para que funcione es conectar la impresora directamente al primer puerto paralelo y establecer las siguientes configuraciones para el puerto paralelo en la BIOS:

- Dirección E/S 378 (hexadecimal)
- Interrupt no es importante
- Modo Normal, SPP o bien Output-Only

- No se utiliza DMA.

Si a pesar de esto no se puede acceder a la impresora a través del primer puerto paralelo, se debe introducir la dirección E/S correspondiente a la configuración de la BIOS de manera explícita con la forma 0x378 en las configuraciones detalladas del puerto paralelo. Si hay dos puertos paralelos disponibles configurados con las direcciones E/S 378 y 278 (hexadecimal), se deben introducir con la forma 0x378, 0x278. Véase la sección *Puertos paralelos* en la página 140.

Nombre de la cola de impresión Puesto que a menudo al imprimir se debe escribir el nombre de la cola de impresión, es recomendable que este nombre sea corto y esté compuesto sólo de minúsculas y de números.

Controladores Ghostscript o lenguaje de impresión (modelo de impresora)

El controlador Ghostscript y el lenguaje de impresión vienen dados por el modelo de impresora correspondiente y se determinan en función de la selección de una configuración predeterminada adecuada para ese modelo de impresora. Esta configuración se puede personalizar en una máscara especial – al seleccionar el fabricante y modelo es cuando de hecho se selecciona el lenguaje de impresión o un controlador Ghostscript con una configuración predefinida adecuado para la impresora.

El controlador Ghostscript es el que genera los datos específicos para impresoras que no tienen soporte para PostScript. Por consiguiente la configuración del controlador Ghostscript es el punto decisivo para definir el tipo de impresión. La selección del controlador GhostScript y la configuración específica del controlador adecuado es lo que determina la imagen de impresión. Aquí es donde se definen las diferencias de la imagen de impresión entre las diferentes configuraciones para la misma impresora.

Si YaST ha detectado automáticamente el modelo de su impresora o bien el modelo existe en la base de datos de impresoras, se realiza una preselección razonable de los controladores Ghostscript adecuados. En este caso, YaST suele proporcionar varias configuraciones predeterminadas – p. ej.

- Impresión en blanco y negro
- Impresión en color 300 dpi
- Calidad fotográfica 600 dpi

Una configuración predeterminada contiene el controlador Ghostscript apropiado y las configuraciones específicas del controlador para un tipo determinado de impresión.

Si existen configuraciones específicas del controlador, estas pueden personalizarse mediante una máscara especial. La relación entre el valor seleccionado y las posibles opciones de una selección subordinada puede distinguirse por la sangría de las entradas del menú. No todas las combinaciones seleccionables de las diferentes configuraciones del controlador funcionan con todos los modelos de impresora; especialmente en combinación con resoluciones altas.

Es imprescindible realizar una comprobación imprimiendo la página de prueba de Y&ST. Si el resultado de esta impresión es incorrecto (p. ej. muchas páginas casi vacías) puede parar la impresión inmediatamente sacando todo el papel y pulsando después el botón 'Parar'. Pero en algunos casos no es posible realizar después otra impresión, con lo cual es menos problemático pulsar el botón 'Parar' y esperar a que la impresión termine.

Si el modelo de la impresora no se encuentra en la base de datos de impresoras, existe una serie de controladores Ghostscript genéricos para los lenguajes de impresión estándar. Éstos se encuentran bajo un "fabricante" genérico.

Algunas configuraciones especiales En cuanto a las configuraciones especiales, deberían dejarse las opciones predeterminadas en caso de duda.

En el sistema de impresión *CUPS* existen las siguientes configuraciones especiales:

- Restricciones de acceso para determinados usuarios.
- Estado de la cola de impresión: Si se ha realizado la impresión o no, y si la cola de impresión debe aceptar las tareas de impresión o no.
- Páginas de cubierta y de corrección: Si se debe imprimir, en qué momento, y qué páginas de cubierta o de corrección deben imprimirse.

En el sistema de impresión *LPRng/lpdfilter* existen las siguientes configuraciones especiales independientes del hardware:

- Se puede fijar aquí la disposición de las hojas para la impresión de textos ASCII, pero no para gráficos y documentos creados con aplicaciones especiales.
- Se puede configurar una cola de impresión *ascii* para casos especiales. Para este tipo de colas *ascii* se fuerza al filtro de impresión a realizar la impresión como texto ASCII. Esto es necesario para forzar

la impresión en texto ASCII de archivos de texto ASCII no reconocidos como tales por el filtro de impresión (p. ej. para imprimir textos fuente de PostScript).

- La codificación específica de cada país afecta a la representación de signos especiales específicos de cada país al imprimir textos ASCII, así como a la representación de texto sencillo de páginas HTML de Netscape.

Configuración para aplicaciones

Los programas de aplicación utilizan las colas de impresión disponibles para imprimir desde la línea de comandos. Por lo tanto, en las aplicaciones no es necesario configurar la impresora sino las colas de impresión existentes.

Se puede imprimir desde la línea de comandos introduciendo:

```
lpr -Pcolor  
⟨nombre_archivo⟩
```

Aquí debe sustituir *⟨nombre_archivo⟩* por el nombre del archivo que quiere imprimir. Con la opción *-P* puede determinar explícitamente la cola de impresión a la que quiere enviarlo. Por ejemplo, con *-Pcolor* se utilizará la cola de impresión *color*.

Configuración manual de puertos locales

Puertos paralelos

En un sistema Linux la conexión a una impresora suele ocurrir a través de un puerto paralelo. El acceso a estas impresoras se produce a través del subsistema *parport* del kernel. La configuración básica de un puerto paralelo con YAST se describe en la sección [Configuración manual](#) en la página 137, por lo que aquí sólo se incluirá información general:

Los puertos paralelos se dan a conocer al subsistema *parport* al cargar los módulos del kernel específicos de la arquitectura. De esta forma es posible trabajar con varios dispositivos *simultáneamente* (p. ej. una unidad ZIP de puerto paralelo y una impresora) conectados a través de *un solo* puerto paralelo. La numeración de archivos de dispositivos para impresoras de puerto paralelo comienza con */dev/lp0*. Para poder imprimir a través del primer puerto

paralelo, se deben cargar los siguientes módulos en el kernel estándar de SuSE: `parport`, `parport_pc` y `lp`. De esto suele encargarse automáticamente el cargador de módulos del kernel ((ingl. *Kernel Module Loader*)) `kmod` tan pronto como se accede a los archivos de dispositivo (p. ej. `/dev/lp0`) por primera vez.

Cuando el módulo `parport_pc` del kernel se carga sin parámetros especiales, intenta detectar y configurar automáticamente los puertos paralelos. En pocas ocasiones no lo consigue y el sistema se "cuelga". En este caso, se debe configurar manualmente e introducir explícitamente los parámetros correctos para `parport_pc`. Por eso se puede impedir la detección automática de impresoras por parte de YaST tal y como se explica en la sección [Configuración de impresoras con YaST](#) en la página 134.

Configuración manual de los puertos paralelos

El puerto paralelo `/dev/lp0` se configura mediante una entrada en `/etc/modules.conf` (archivo [Configuración manual de los puertos paralelos](#) en esta página).

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=none
```

Fichero 4: /etc/modules.conf: primer puerto paralelo

En `io` aparece la dirección de entrada y salida del puerto paralelo y en `irq` aparece `none` como configuración predeterminada para el modo de operación "polling"; también puede aparecer la interrupción del puerto paralelo. El modo "polling" es menos problemático que el modo de interrupciones ya que se evitan los conflictos de interrupciones. Sin embargo existen placas bases o impresoras que sólo funcionan correctamente en modo de interrupciones. Además este modo permite a la impresora recibir datos suficientes en momentos de sobrecarga del sistema.

Para que estas opciones funcionen, hace falta configurar los siguientes valores (siempre que existan) para el puerto paralelo en la BIOS del ordenador o mediante el firmware:

- Dirección entrada/salida 378 (hexadecimal)
- Interrupt 7 (no importa en modo "polling")
- Modo Normal, SPP o bien Output-Only (los demás modos no funcionan siempre).
- DMA está desactivado (por defecto en modoNormal)

Si la interrupción 7 aún está libre, se puede activar el funcionamiento de interrupciones con la entrada en el archivo [Configuración manual de los puertos paralelos](#) en esta página

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

Fichero 5: /etc/modules.conf: modo de interrupciones para el primer puerto paralelo

Antes de que el modo de interrupciones esté activado, el archivo `/proc/interrupts` permite averiguar qué interrupciones ya se están utilizando. Aquí sólo se muestran las interrupciones que se encuentren funcionando en este momento; lo que puede cambiar en función del hardware que se esté usando. No se debe utilizar la interrupción del puerto paralelo de otro modo. En caso de duda, lo mejor es tomar el modo polling

Activación y prueba de un puerto paralelo

El puerto paralelo está disponible tras reiniciar el ordenador. En lugar de reiniciar la máquina, basta con actualizar como usuario `root` la lista de las dependencias de módulos y descargar los módulos de kernel que se comunican con el puerto paralelo...

```
depmod -a 2>/dev/null
rmmod lp
rmmod parport_pc
rmmod parport
```

...para cargarlos nuevamente:

```
modprobe parport
modprobe parport_pc
modprobe lp
```

Si la impresora es capaz de imprimir texto ASCII, el usuario SuSE `root` ha de poder imprimir una página con la palabra `Hello` mediante el siguiente comando:

```
echo -en "\rHello\r\f" >/dev/lp0
```

Aquí, la palabra `Hello` está preparada para la impresión, encontrándose entre el carácter ASCII `\r` que representa el retorno de carro, y el carácter ASCII `\f` que provoca un salto de página.

Puerto USB

La BIOS del ordenador debe tener una interrupción activada para USB. Para ello, en el caso de una BIOS Award es necesario fijar la entrada 'USB IRQ' como Enabled en el menú 'PNP AND PCI SETUP'. Según la versión de la BIOS, pueden emplearse otras denominaciones.

Para probar si se puede acceder a la impresora USB, teclee como usuario root:

```
echo -en "\rHello\r\f" >/dev/usb/lp0
```

Suponiendo que sólo haya una impresora USB conectada y que esta impresora pueda imprimir texto ASCII, deberá salir impresa una página con la palabra Hello.

Algunas impresoras USB requieren una secuencia especial de control antes de aceptar los datos USB. Puede encontrar más información sobre este tema introduciendo "Epson" y "usb" como palabras clave en nuestra base de datos de soporte <http://sdb.suse.de/es/sdb/html>.

Por lo general, tras introducir el siguiente comando debería aparecer el fabricante y la descripción del producto:

```
cat /proc/bus/usb/devices
```

Si no es así, puede ser debido a uno de los siguientes motivos:

- El sistema USB (aún) no ha detectado el dispositivo— quizás porque la impresora USB está apagada y por tanto no se puede establecer contacto con ella.
- El sistema USB ha detectado el dispositivo pero no conoce ni el fabricante ni la descripción del producto, por lo que no muestra nada. Sin embargo sí es posible comunicarse con la impresora.

A veces sucede que la impresora deja de responder (p. ej. por haber sacado el enchufe USB durante la impresión). Normalmente debería bastar con utilizar los siguientes comandos para reiniciar el sistema USB:

```
rchotplug stop  
rchotplug start
```

Si esto no ayuda, se pueden finalizar todos los procesos que acceden a /dev/usb/lp0 y descargar y cargar nuevamente todos los módulos de kernel relacionados con la impresora USB. Previamente se debe comprobar con `lsmod` qué

módulos USB están cargados (`usb-uhci`, `usb-ohci` o bien `uhci`) y si existen otras dependencias entre módulos. Por ejemplo, la salida siguiente muestra que el módulo `usbcore` es requerido por los módulos `printer` y `usb-uhci`:

```
usbcore ... [printer usb-uhci]
```

Por este motivo, aquí es necesario descargar los módulos `printer` y `usb-uhci` antes del módulo `usbcore`. Introduzca para ello los siguientes comandos como usuario `root` (dependiendo del sistema, `usb-uhci` puede ser también `uhci` o `usb-ohci`):

```
fuser -k /dev/usb/lp0
rchtplug stop
rmmod printer
rmmod usb-uhci
umount usbdevfs
rmmod usbcore
modprobe usbcore
mount usbdevfs
modprobe usb-uhci
modprobe printer
rchtplug start
```

Si hay más de una impresora conectada, se debe tener en cuenta lo siguiente: El subsistema USB reconoce automáticamente las impresoras USB conectadas. Nos podemos comunicar con la primera impresora USB detectada mediante el dispositivo `/dev/usb/lp0` y con la segunda impresora USB detectada mediante el dispositivo `/dev/usb/lp1`. Dependiendo del modelo de impresora puede que también se detecten impresoras apagadas. Esto es debido a que también es posible comunicarse con algunas impresoras en estado de apagado a través del puerto USB. Para evitar una confusión entre dispositivos USB, se debería encender todas las impresoras USB antes de arrancar Linux y dejarlas encendidas en la medida de lo posible durante el funcionamiento del sistema.

Puerto IrDA

Es una emulación de un puerto paralelo a través de una conexión de infrarrojos. El controlador en el kernel de Linux ofrece un puerto paralelo simulado en el dispositivo `/dev/ir_lpt0`. Es posible comunicarse con una impresora a través de un puerto de infrarrojos de la misma forma que a través de un puerto paralelo; la única diferencia es que se utilizará `/dev/ir_lpt0` en vez de `/dev/lp0`.

Compruebe si es posible comunicarse con la impresora IrDA introduciendo como usuario `root`:

```
echo -en "\rHello\r\f" >/dev/irllpt0
```

Suponiendo que la impresora pueda imprimir texto ASCII, debería imprimirse una página con la palabra `He llo`.

En cualquier caso, la impresora debe aparecer en la salida del comando `irdadump`. Si este comando no existe, es necesario instalar el paquete `irda`. Si la impresora no se muestra tras ejecutar `irdadump`, es que no es posible comunicarse con ella. Si no aparece nada de ninguna manera, lo más probable es que no se haya iniciado el servicio del sistema IrDA, puesto que este no se activa automáticamente al arrancar el ordenador. El sistema IrDA puede iniciarse y pararse con

```
rcirda start  
rcirda stop
```

Puertos serie

El funcionamiento de una impresora conectada al puerto serie está explicado para el spooler LPRng en *LPRng-Howto* en <file:///usr/share/doc/packages/lprng/LPRng-HOWTO.html>, y en particular en <file:///usr/share/doc/packages/lprng/LPRng-HOWTO.html#SECSERIAL> y en página del manual de `printcap` (`man printcap`). También puede encontrar más información en la base de datos de soporte introduciendo la palabra clave “serie”.

Configuración manual de LPRng/lpfilter

Normalmente se configura el sistema de impresión con YaST tal y como se indica en la sección *Configuración de impresoras con YaST* en la página 134. Adicionalmente existe para el sistema de impresión LPRng/lpfilter el programa `lprsetup`. La funcionalidad completa de `lprsetup` es accesible desde la línea de comandos.

Al configurar una impresora con YaST, éste se encarga de recopilar la información necesaria y de activar `lprsetup` con las opciones precisas para configurar el sistema de impresión LPRng/lpfilter.

El programa `lprsetup` está concebido como una herramienta para “expertos”. Al contrario que YaST, no ayuda al usuario a encontrar los valores adecuados para las diferentes opciones. Con `lprsetup -h` se mencionan brevemente las

distintas opciones. página del manual de `lprsetup` (`man lprsetup`) y página del manual de `lpdfilter` (`man lpdfilter`) proporcionan más información. Puede obtener más información sobre los controladores Ghostscript y parámetros específicos de los diferentes controladores en las secciones *Determinar el controlador de impresión correcto* en la página 130 y *Acerca de Ghostscript* en la página 173.

El spooler de impresión LPRng

Como spooler de impresión estándar del sistema de impresión LPRng/`lpdfilter` se utiliza LPRng (paquete `lprng`).

El spooler de impresión `lpd` (ingl. *Line Printer Daemon*) se activa automáticamente mediante el script `/etc/init.d/lpd` al arrancar el sistema. Este spooler de impresión se ejecuta como daemon en segundo plano y se puede iniciar y parar manualmente con:

```
rclpd start
rclpd stop
```

Los archivos de configuración para el paquete LPRng son:

/etc/printcap Configuración de cada cola de impresión

/etc/lpd.conf Configuración global del spooler

/etc/lpd.perms Configuración de los permisos de acceso

Con `rclpd start` también se activa `checkpc -f` en conformidad con `/etc/init.d/lpd`. `checkpc -f` crea los directorios de spool `/var/spool/lpd/*` en función de las entradas en `/etc/printcap` y adapta los permisos de acceso.

Cuando el spooler de impresión se inicia, se sirve de las entradas en `/etc/printcap` para averiguar qué colas de impresión están definidas. Su trabajo es organizar la impresión de los trabajos ((ingl. *jobs*)) en la cola:

- Administra las colas de impresión locales y envía los archivos de datos de un trabajo directamente a la impresora o a otra cola de espera, pudiendo utilizar también un filtro de impresión entre medias.
- Tiene en cuenta el orden de los trabajos en las colas de impresión.
- Vigila el estado de las colas de impresión y de la impresora y proporciona información sobre las mismas.

- Admite o rechaza solicitudes de impresión de máquinas remotas dirigidas a colas locales en el puerto 515.
- Reenvía solicitudes de impresión en colas remotas al spooler de impresión de la máquina remota (es decir, al puerto 515 de dicha máquina).

Puede obtener información detallada sobre el spooler LPRng en *LPRng-Howto* en <file:///usr/share/doc/packages/lprng/LPRng-HOWTO.html> en página del manual de `printcap` (`man printcap`) y en página del manual de `lpd` (`man lpd`).

Imprimir desde aplicaciones

Los programas de aplicación imprimen con el comando `lpr`. Seleccione para ello en la aplicación el nombre de una cola de impresión existente (p. ej. `color`) o introduzca en el diálogo de impresión de la aplicación el comando correspondiente (p. ej. `lpr -Pcolor`).

Para imprimir desde la línea de comandos se utiliza el comando `lpr -Pcolor <archivo>`. Aquí debe sustituirse `<archivo>` por el nombre del archivo que se va a imprimir. La opción `-P` permite definir explícitamente la cola de impresión. Así por ejemplo, con `lpr -Pcolor archivo` se usa la cola de impresión `color`.

Herramientas de línea de comandos para LPRng

Las herramientas de la línea de comandos se describen con detalle en *LPRng-Howto* en <file:///usr/share/doc/packages/lprng/LPRng-HOWTO.html#LPRNGCLIENTS>, por lo que aquí sólo presentamos una breve recopilación.

Para colas de impresión locales

Generar trabajos de impresión

El comando `lpr` está explicado en *LPRng-Howto* en <file:///usr/share/doc/packages/lprng/LPRng-HOWTO.html#LPR>, a continuación una mera información general:

Normalmente se imprime mediante `lpr -P <cola_impresión> <archivo>`. Si se omite la opción `-P<cola_impresión>`, se usa como valor predeterminado el contenido de la variable de entorno `PRINTER`. Lo mismo vale también para los comandos `lpq` y `lprm` — ver también página del manual de `lpr` (`man lpr`), página del manual de `lpq` (`man lpq`) y página del manual de `lprm` (`man lprm`). Al arrancar se fija automáticamente la variable de entorno `PRINTER`. Esta variante puede mostrarse con el comando `echo $PRINTER` y cambiarse a otra cola de impresión con `export PRINTER=<cola_impresión>`.

Mostrar el estado

`lpq -P<cola_impresión>` muestra los trabajos de impresión que se encuentran en la cola de impresión indicada. Si en el spooler `LPRng` se indica `all` (todas) como cola de impresión, se mostrarán todos los trabajos de todas las colas.

Con `lpq -s -P<cola_impresión>` se muestra una cantidad mínima de información mientras que con `lpq -l -P<cola_impresión>` se muestra una cantidad mayor.

Con `lpq -L -P<cola_impresión>` se mostrará un detallado informe del estado, de gran ayuda para el diagnóstico de problemas.

Puede encontrar más información en la sección *Mostrar el estado de colas de impresión remotas* así como en página del manual de `lpq` (`man lpq`) y <file:///usr/share/doc/packages/lprng/LPRng-HOWTO.html#LPQ> en *LPRng-Howto*.

Eliminar trabajos de impresión

`lprm -P<cola_impresión> <número_trabajo>` elimina la tarea de impresión que tenga el número indicado en la cola especificada, siempre que la tarea pertenezca al usuario que ha ejecutado el comando `lprm`. Un trabajo de impresión pertenece al usuario del ordenador que lo ha generado. Para saber quién es este usuario y qué número se le ha asignado a ese trabajo, utilice el comando `lpq`.

Con el comando `lprm -Pall all` se eliminarán todos los trabajos de todas las colas de impresión que pertenezcan al usuario que ha introducido el comando `lprm`. El usuario `root` puede eliminar todas las tareas (de todas las colas).

Puede obtener más información en página del manual de `lprm` (`man lprm`) y <file:///usr/share/doc/packages/lprng/LPRng-HOWTO.html#LPRM> en *LPRng-Howto*.

Control de las colas de impresión

El comando `lpc option <cola_impresión>` muestra el estado de las colas indicadas y permite modificarlas. Las opciones más importantes son:

`help` explica brevemente todas las posibles opciones

`status <cola_impresión>` informa sobre el estado de la cola.

`disable <cola_impresión>` deja de aceptar nuevos trabajos en la cola de impresión.

`enable <cola_impresión>` reanuda la impresión de los trabajos en la cola.

`stop <cola_impresión>` detiene la impresión de los trabajos de la cola; la tarea que se está imprimiendo se termina de imprimir.

`start <cola_impresión>` reanuda la impresión de los trabajos en la cola.

`down <cola_impresión>` actúa como `disable` más `stop`.

`up <cola_impresión>` tiene el mismo efecto que `enable` añadiéndole `start`.

`abort <cola_impresión>` actúa como `down`, con la diferencia de que detiene inmediatamente un trabajo que se esté imprimiendo. Los trabajos se mantienen y es posible reanudarlos después del reinicio de la cola (`up`).

Para modificar las colas de impresión necesita permisos de `root`. Estos comandos se pueden introducir directamente en la línea de comandos (p. ej. `lpc status all`) o bien ejecutar `lpc` sin parámetros. En el último caso se abre un cuadro de diálogo con su propio (ingl. *Prompt*) `lpc>` a la espera de que se introduzcan las opciones mencionadas arriba. Con `quit` o `exit` se sale de esta ventana.

Si por ejemplo la salida de `lpc status all` es:

Printer	Printing	Spooling	Jobs	Server	Subserver
lp@earth	enabled	enabled	2	123	456
color@earth	disabled	disabled	0	none	none
laser@earth	disabled	enabled	8	none	none

indica que la cola `lp` está en funcionamiento y contiene dos trabajos de impresión (uno de ellos ya se está imprimiendo). La cola `color` está totalmente apagada. La cola `laser` no puede imprimir p. ej. debido a trabajos de reparación

temporales, pero permite que se generen tareas de impresión, que se van acumulando en la cola (8 en este caso).

Puede obtener información adicional en página del manual de `lpc` (`man lpc`) y <file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#LPC> en *LPRng-Howto*.

Para colas de impresión remotas

Se sustituye `<servidor_impresión>` por el nombre o dirección IP del servidor de impresión y `<cola_impresión>` debe ser una cola del servidor de impresión.

Generar trabajos de impresión

El spooler LPRng permite acceder directamente a colas remotas mediante el comando `lpr`:

```
lpr -P<cola_impresión>@<servidor_impresión> <archivo>.
```

Mostrar el estado

Con los siguientes comandos se puede inspeccionar el estado de una cola de impresión remota:

```
lpq -P<cola_impresión>@<servidor_impresión>
lpq -s -P<cola_impresión>@<servidor_impresión>
lpq -l -P<cola_impresión>@<servidor_impresión>
lpq -L -P<cola_impresión>@<servidor_impresión>

y

lpc status <cola_impresión>@<servidor_impresión>
lpc status all@<servidor_impresión>
```

Especialmente con `lpq -s -Pall@<servidor_impresión>` o con `lpc status all@<servidor_impresión>` se puede solicitar el nombre de todas las colas en dicho servidor de impresión, siempre que LPRng se utilice también en el servidor.

Esto puede ser útil sobre todo cuando resulte imposible imprimir en la cola remota. Con `lpq -L -P<cola_impresión>@<servidor_impresión>` se muestra un informe detallado del estado para realizar un diagnóstico a distancia, siempre que en el servidor de impresión se use LPRng.

Eliminar trabajos de impresión

Con los siguientes comandos es posible eliminar todos los trabajos de impresión en colas remotas creadas por Vd. mismo:

```
lprm -P<cola_impresión>@<servidor_impresión> <número_trabajo>
lprm -P<cola_impresión>@<servidor_impresión> all
lprm -Pall@<servidor_impresión> all
```

root no posee ningún permiso especial en colas remotas. La variable `all` sólo funciona cuando se utiliza LPRng en el servidor de impresión.

Resolución de problemas con los comandos anteriores en LPRng

Los trabajos de impresión permanecen en las colas de impresión cuando, en medio de la impresión, el ordenador se para y es necesario reiniciar Linux; – si un trabajo causa problemas, elimínelo de la cola con los comandos descritos anteriormente.

En caso de averías en la comunicación entre el ordenador y la impresora, ésta no puede interpretar correctamente los datos obtenidos y puede ocurrir que acabe imprimiendo una gran cantidad de páginas llenas de signos ininteligibles.

1. Primero retire todo el papel en las impresoras a chorro de tinta o abra la bandeja del papel en impresoras láser para que la impresión se detenga.
2. Puesto que el trabajo de impresión sólo desaparecerá de la cola después de haber sido enviado por completo a la impresora, lo más probable es que aún aparezca en la cola. Compruebe con `lpq` o `lpc status` desde qué cola se está imprimiendo y elimine con `lprm` el trabajo correspondiente.
3. Puede que se hayan enviado algunos datos a la impresora a pesar de que el trabajo ya no esté en la cola. Con el comando `fuser -k /dev/lp0` para una impresora en puerto paralelo o `fuser -k /dev/usb/lp0` para una impresora USB, se pueden parar todos los procesos relacionados con la impresora.
4. Desconecte la impresora durante unos minutos. Después vuelva a colocar el papel y encienda la impresora.

El filtro de impresión del sistema

LPRng/lpfilter

Como filtro de impresión se usa `lpfilter` (paquete `lpfilter`). A continuación se describe de forma detallada el desarrollo de un trabajo de impresión. Para un análisis exacto del filtro de impresión, revise los scripts del filtro de impresión (de forma especial `/usr/lib/lpfilter/bin/if`) y en caso necesario siga los pasos descritos en el apartado [Búsqueda de errores en lpfilter](#) en la página 160.

1. El filtro de impresión (`/usr/lib/lpfilter/bin/if`) analiza las opciones que le pasa directamente el spooler de impresión o bien las lee del "control file" (archivo de control) del trabajo de impresión y de los archivos `/etc/printcap` y `/etc/lpfilter/<cola_impresión>/conf` (`cola_impresión` debe sustituirse por el verdadero nombre de la cola de impresión).
2. Si se trata una cola `ascii`, el filtro de impresión se ve forzado a manejar los datos que se van a imprimir como si fueran texto ASCII. Si no es una cola `ascii`, el filtro de impresión intenta determinar automáticamente el tipo de datos del que se trata. Con este fin, el script `/usr/lib/lpfilter/bin/guess` aplica el comando `file` a los datos que se van a imprimir. El tipo de datos a imprimir se determina mediante la salida de este comando y las entradas en el archivo `/etc/lpfilter/types`.
3. Dependiendo del tipo de datos a imprimir y de la cola, se efectúa una conversión posterior en datos específicos para la impresora:
 - Si se trata de una cola `raw`, los datos a imprimir se reenvían directamente a la impresora (o a otra cola). No obstante, dependiendo de la configuración en `/etc/lpfilter/<cola_impresión>/conf`, puede efectuarse una recodificación sencilla con `recode`. Para una cola `raw` pura – es decir completamente sin `lpfilter` – es necesario eliminar la línea `:if=/usr/lib/lpfilter/bin/if:\ de /etc/printcap` en la cola correspondiente.
 - Si no se trata de una cola `raw`:
 - a) Si los datos a imprimir no son del tipo PostScript, se convierten a PostScript ejecutando `/usr/lib/lpfilter/filter/typ2ps` (aquí debe sustituirse `typ` por el tipo verdadero de datos a imprimir). Sobre todo el texto ASCII ha de convertirse a PostScript conforme a `/usr/lib/lpfilter/filter/`

ascii2ps con el programa a2ps. De esta forma se convierte a PostScript la codificación regional definida para la cola de impresión, para así poder imprimir correctamente los caracteres especiales específicos de un país en texto plano; ver también página del manual de a2ps (man a2ps).

- b) En caso necesario se pueden formatear otra vez los datos PostScript, siempre que exista un script correspondiente en `/etc/lpfilter/<cola_impresión>/pre` (aquí debe sustituirse `<cola_impresión>` por el verdadero nombre de la cola).
- c) Dado el caso, los datos PostScript son convertidos a otro lenguaje de impresión.
 - Si la impresora conectada tiene soporte PostScript, los datos PostScript son enviados directamente a la impresora (o a algunas de las otras colas). Si es necesario se activan las funciones bash "duplex" y "tray", definidas en `/usr/lib/lpfilter/global/functions`, para habilitar la impresión dúplex y la selección de la bandeja de alimentación de papel a través de comandos PostScript. Para ello es necesario que la impresora PostScript sea capaz de procesar estos comandos correctamente.
 - Si la impresora conectada no tiene soporte PostScript, se emplea Ghostscript con un controlador Ghostscript adecuado para el lenguaje de impresión de la impresora usada, con el fin de generar los datos específicos para dicha impresora. Estos últimos son enviados finalmente a la impresora (o a una cola).
 Los parámetros para ejecutar Ghostscript están guardados en `/etc/printcap` directamente en la línea `cm` o bien en el archivo `/etc/lpfilter/<cola_impresión>/upp` (aquí debe sustituirse `<cola_impresión>` por el verdadero nombre de la cola).
 En caso necesario es posible formatear nuevamente la salida de Ghostscript siempre que exista un script adecuado en `/etc/lpfilter/<cola_impresión>/post` (aquí debe sustituirse `<cola_impresión>` por el verdadero nombre de la cola).
- d) Los datos específicos para la impresora son enviados a la impresora (o a una cola). Tanto delante como detrás de los datos específicos para la impresora se pueden enviar secuencias de control específicas para la impresora siempre y cuando hayan sido introducidas en `/etc/lpfilter/<cola_impresión>/conf`.

Configuración de lpdfilter

Al configurar el sistema de impresión con YoST como se describe en [Configuración de impresoras con YoST](#) en la página 134, se configura también normalmente el filtro de impresión lpdfilter.

Para realizar configuraciones especiales hay que editar manualmente los archivos de configuración del filtro de impresión. Cada cola de impresión tiene su propio archivo de configuración `/etc/lpdfilter/<cola_impresión>/conf` (aquí debe sustituirse `<cola_impresión>` por el verdadero nombre de la cola), que también contiene informaciones sobre cada opción.

Complementos para lpdfilter

1. Si los datos a imprimir no son del tipo PostScript, normalmente son convertidos a PostScript mediante la ejecución de `/usr/lib/lpdfilter/filter/typ2ps` (aquí se debe sustituir `typ` por el tipo de datos a imprimir).

Si se guarda un script adecuado en `/etc/lpdfilter/<cola_impresión>/typ2ps`, éste se utiliza para convertir los datos a imprimir a PostScript. Este script recibe los datos a imprimir a través de `stdin` y debe producirlos en PostScript a través de `stdout`

2. Dado el caso se pueden formatear los datos PostScript otra vez, siempre que exista un script adecuado en `/etc/lpdfilter/<cola_impresión>/pre`. También es posible cargar los PostScript-Preloads propios con un script adecuado. Este script obtiene datos PostScript de `stdin` y tiene que producir PostScript a través de `stdout`. paquete `psutils` contiene programas para reformatear datos PostScript. Sobre todo el programa `pstops` ofrece amplias posibilidades para reformatear; ver también página del manual de `pstops` (`man pstops`).
3. Parámetros especiales de Ghostscript: Al configurar con YoST los parámetros para la activación de Ghostscript se guardan en el archivo `/etc/lpdfilter/<cola_impresión>/upp` (aquí debe sustituirse `<cola_impresión>` por el verdadero nombre de la cola). Este archivo se puede editar manualmente y añadir en él parámetros especiales. Para más información sobre los parámetros Ghostscript consulte el apartado [Acerca de Ghostscript](#) en la página 173.
4. Existe la posibilidad de formatear otra vez la salida de Ghostscript, siempre que exista un script adecuado en `/etc/`

`lpdfilter/⟨cola_impresión⟩/post` (aquí debe sustituir `⟨cola_impresión⟩` por el verdadero nombre de la cola). Este script obtiene la salida de Ghostscript a través de `stdin` y debe producir datos específicos para la impresora a través de `stdout`.

Un ejemplo independiente del hardware

Supongamos que existe una cola de impresión `test` en la que debe imprimirse texto ASCII con los números de línea antepuestos. Además siempre han de imprimirse dos páginas reducidas en una hoja. Para conseguirlo se podrían crear los scripts `/etc/lpdfilter/test/ascii2ps` y `/etc/lpdfilter/test/pre`.

```
#!/bin/bash
cat -n - | a2ps -1 --stdin=' ' -o -
```

Fichero 6: `/etc/lpdfilter/test/ascii2ps`: conversión de ASCII a PostScript

```
#!/bin/bash
pstops -q '2:0L@0.6(20cm,2cm)+1L@0.6(20cm,15cm)'
```

Fichero 7: `/etc/lpdfilter/test/pre`: reformatear PostScript

Estos scripts deben ser ejecutables para todos los usuarios, lo cual se puede conseguir utilizando `chmod`.

```
chmod -v a+rx /etc/lpdfilter/test/ascii2ps
chmod -v a+rx /etc/lpdfilter/test/pre
```

El comando `pstops` funciona sólo para archivos PostScript creados de tal forma que sea posible reformatearlos (es el caso habitual).

Usar PostScript-Preloads propios

Los PostScript-Preloads son pequeños archivos PostScript que contienen comandos especiales y que se activan antes de los auténticos datos de impresión para iniciar correctamente impresoras PostScript o Ghostscript conforme a estos comandos especiales. En general, los PostScript-Preloads se usan para activar la impresión dúplex o el uso de determinados alimentadores en impresoras PostScript, o bien configurar la corrección gamma y el ajuste de los márgenes.

Para ello es preciso que GhostScript o bien la impresora PostScript puedan procesar adecuadamente los comandos especiales de PostScript indicados abajo (Ghostscript no reacciona a los comandos para la impresión dúplex o para definir la bandeja de alimentación).

En la siguiente configuración se supone que la cola correspondiente se llama test.

Impresión duplex Para habilitar y deshabilitar la impresión dúplex puede crear los archivos /etc/lpfilter/test/duplexon.ps y/etc/lpfilter/test/duplexoff.ps:

```
%!PS
statusdict /setduplexmode known
{statusdict begin true setduplexmode end} if {} pop
```

Fichero 8: /etc/lpfilter/test/duplexon.ps: habilitar la impresión dúplex

```
%!PS
statusdict /setduplexmode known
{statusdict begin false setduplexmode end} if {} pop
```

Fichero 9: etc/lpfilter/test/duplexoff.ps: deshabilitar la impresión dúplex

Para girar 180 grados el reverso de la hoja en la impresión dúplex, puede utilizar el siguiente código PostScript:

```
%!PS
statusdict /setduplexmode known
{statusdict begin true setduplexmode end} if {} pop
statusdict /set tumble known
{statusdict begin true set tumble end} if {} pop
```

Selección de la bandeja del papel Para activar la bandeja estándar con el número 0 ó p.ej. la bandeja con el número 2, puede crear los archivos /etc/lpfilter/test/tray0.ps y /etc/lpfilter/test/tray2.ps:

```
%!PS
statusdict /setpapertray known
{statusdict begin 0 setpapertray end} if {} pop
```

Fichero 10: /etc/lpfilter/test/tray0.ps: activar bandeja 0


```

%!PS
statusdict /setpapertray known
{statusdict begin 2 setpapertray end} if {} pop

```

Fichero 11: /etc/lpdfilter/test/tray2.ps: activar bandeja 2

Ajuste de los márgenes Para modificar la configuración de los márgenes puede crear el archivo /etc/lpdfilter/test/margin.ps:

```

%!PS
<<
/.HWMargins [left bottom right top]
/PageSize [width height]
/Margins [left-offset top-offset]
>>
setpagedevice

```

Fichero 12: /etc/lpdfilter/test/margin.ps: ajuste de márgenes

Los valores de los márgenes `left`, `bottom`, `right` y `top` y del tamaño de la hoja `width` y `height` se indican en puntos, equivaliendo el tamaño de un punto a 1/72 de pulgada (unos 0,35 mm). Los desplazamientos `left-offset` y `top-offset` se especifican en cambio en puntos raster, con lo cual dependen de la resolución respectiva.

Para mover la posición de la impresión en la hoja se utiliza el archivo /etc/lpdfilter/test/offset.ps

```

%!PS
<< /Margins [left-offset top-offset] >> setpagedevice

```

Fichero 13: /etc/lpdfilter/test/offset.ps: posición de la impresión

Corrección gamma Para ajustar el brillo de los colores puede crear los archivos /etc/lpdfilter/test/cmyk.ps y /etc/lpdfilter/test/rgb.ps

```

%!PS
{cyan exp} {magenta exp} {yellow exp} {black exp}
setcolortransfer

```

Fichero 14: /etc/lpdfilter/test/cmyk.ps: corrección gamma CMYK

```
%!PS
{red exp} {green exp} {blue exp} currenttransfer
setcolortransfer
```

Fichero 15: /etc/lpdfilter/test/rgb.ps: corrección gamma RGB

El modelo de colores (CMYK o RGB) tiene que ser el adecuado para su impresora. Para averiguar los valores adecuados para cyan, magenta, yellow, black, red, green y blue ha de realizar las pruebas correspondientes. Normalmente, estos valores suelen estar entre 0.001 y 9.999

Suponiendo que trabaja con el sistema X Window, lo puede probar en la pantalla de un terminal introduciendo el siguiente comando: Sin corrección gamma:

```
gs -r60 \
/usr/share/doc/packages/ghostscript/examples/colorcir.ps
```

Con corrección gamma uno de los siguientes ejemplos:

```
gs -r60 /etc/lpdfilter/test/cmyk.ps \
/usr/share/doc/packages/ghostscript/examples/colorcir.ps
gs -r60 /etc/lpdfilter/test/rgb.ps \
/usr/share/doc/packages/ghostscript/examples/colorcir.ps
```

Para terminar pulse (Control) + (C).

Reiniciar la impresora Para devolver la impresora a su estado original puede crear el archivo /etc/lpdfilter/test/reset.ps:

```
%!PS
serverdict begin 0 exitserver
```

Fichero 16: /etc/lpdfilter/test/reset.ps: reinicio de la impresora

Para activar el uso de un archivo PostScript-Preload puede crear el script /etc/lpdfilter/test/pre:

```
#!/bin/bash
cat /etc/lpdfilter/test/preload.ps -
```

Fichero 17: /etc/lpdfilter/test/pre: cargar PostScript-Preload

Aquí debe sustituirse `preload.ps` por el nombre del archivo Preload correspondiente. Además el script debe ser ejecutable y el archivo Preload legible para cualquier usuario. Estos permisos se pueden definir con `chmod`:

```
chmod -v a+rx /etc/lpddfilter/test/pre
chmod -v a+r /etc/lpddfilter/test/preload.ps
```

El mismo mecanismo se puede utilizar para enviar un archivo PostScript no sólo antes, sino también después de enviar los propios datos de impresión PostScript a la impresora. Si desea por ejemplo reiniciar la impresora después de terminar un trabajo, puede completar el script `/etc/lpddfilter/test/pre` de esta forma:

```
#!/bin/bash
cat /etc/lpddfilter/test/preload.ps - /etc/lpddfilter/test/reset.ps
```

Fichero 18: `etc/lpddfilter/test/pre`: PostScript-Preload y PostScript-Reset

Ejemplo de configuración de una impresora GDI

Se debe configurar una cola `gdi` para una impresora GDI. Tales impresoras normalmente no se pueden usar bajo Linux; véase el apartado [La problemática de las impresoras GDI](#) en la página 132 más arriba. Existen controladores especiales para algunas impresoras GDI que sirven de complemento al controlador de Ghostscript. Estos controladores adicionales convierten la salida de Ghostscript al formato específico de la impresora. Hay que mencionar que tales controladores a menudo sólo permiten una impresión limitada—p. ej. sólo impresión en blanco y negro. Ghostscript y el controlador colaboran entonces de la siguiente manera (véase también el apartado [Acerca de Ghostscript](#) en la página 173 más abajo).

1. Ghostscript convierte los datos PostScript en un raster de píxeles individuales. Un controlador GhostScript adecuado para el controlador “acoplado” da como salida datos raster en el formato y la resolución adecuados.
2. El controlador convierte los datos raster en el formato específico de la impresora.

A continuación se supone que existe un controlador de la impresora adecuado para la presente versión de SuSE Linux o bien que lo puede descargar de Internet. Además, este controlador debe funcionar como se ha expuesto arriba y el lector ha de estar familiarizado con el manejo de fuentes Unix (p. ej. con archivos `.zip` o `.tar.gz` o paquetes `.rpm`).

Después de descomprimir tales archivos, normalmente encuentra instrucciones para la instalación en archivos llamados README o INSTALL, o en un subdirectorio doc. Si se trata de un archivo .tar.gz, por regla general hay que compilar e instalar el propio controlador.

A continuación se supone que:

- El controlador es /usr/local/bin/printerdriver.
- Se necesita el controlador Ghostscript pbmraw con una resolución de 600 dpi.
- La impresora está conectada al primer puerto paralelo /dev/lp0.

La documentación del controlador informa sobre qué controlador Ghostscript y qué resolución deben emplear realmente.

Primero hay que crear la cola gdi con lprsetup (como usuario root):

```
lprsetup -add gdi -lprng -device /dev/lp0 \  
-driver pbmraw -dpi 600 -size a4dj -auto -sf
```

A continuación cree el siguiente script /etc/lpfilter/gdi/post:

```
#!/bin/bash /usr/local/bin/printerdriver <parámetros_controlador>
```

En caso necesario hay que indicar los <parámetros_controlador> adecuados. Consulte la documentación del controlador para saber qué parámetros debe aplicar realmente. Hay que modificar los permisos del script a fin de que cualquier usuario pueda ejecutarlo. A continuación se reinicia el spooler de impresión:

```
chmod -v a+rx /etc/lpfilter/gdi/post  
rclpd stop  
rclpd start
```

Ahora cualquier usuario puede imprimir mediante:

```
lpr -Pgdi <archivo>
```

Búsqueda de errores en lpfilter

El grado de depuración adecuado se activa quitando el símbolo de comentario '#' delante de la línea correspondiente en el script principal /usr/lib/lpfilter/bin/if del filtro de impresión.

```
# DEBUG="off"  
# DEBUG="low"  
# DEBUG="medium"  
# DEBUG="high"
```

Fichero 19: /usr/lib/lpfilter/bin/if: grado de depuración

Al indicar `DEBUG="low"` sólo se guarda la salida `stderr` de `/usr/lib/lpfilter/bin/if` en un archivo llamado `/tmp/lpfilter.if-$$`. `XXXXXX` (aquí debe sustituirse `XXXXXX` por una combinación de símbolos aleatoria pero única).

Un valor de `DEBUG="medium"` significa que además se guarda la salida `stderr` de los scripts en `/usr/lib/lpfilter/filter/` ejecutados por `/usr/lib/lpfilter/bin/if`. La salida se guarda en archivos con la forma `/tmp/lpfilter.name-$$`. `XXXXXX` (aquí deben sustituirse `name` por el nombre del script ejecutado y `$$`. `XXXXXX` como se ha descrito arriba).

Con el valor `DEBUG="high"`, además la salida no se envía a la impresora sino que se guarda en un archivo de la forma `/tmp/lpfilter.out-$$`. `XXXXXX` (aquí debe sustituirse `$$`. `XXXXXX` como ya se ha descrito).

Para no perder la orientación, es recomendable eliminar estos archivos con `rm -v /tmp/lpfilter*` antes de iniciar una prueba nueva.

El sistema de impresión CUPS

Convenciones lingüísticas

Con *cliente* o *programa cliente* se indica un programa que es iniciado para enviar trabajos de impresión al daemon de impresión. Un *daemon de impresión* es un servicio local que acepta trabajos de impresión, que luego reenvía o procesa él mismo. Un *servidores* un daemon que puede enviar datos a una o más impresoras. Cada servidor tiene simultáneamente la funcionalidad de un daemon. En la mayoría de los casos ni los usuarios ni los desarrolladores de CUPS distinguen especialmente entre los conceptos *servidor* y *daemon*.

IPP y servidor

Los trabajos de impresión se envían con programas basados en CUPS como `lpr`, `kprinter` o `xpp`, y con ayuda de IPP, *Internet Printing Protocol* (Protocolo de Impresión de Internet). IPP está definido en los estándares de Internet RFC-2910 y RFC-2911 (véase <http://www.rfc-editor.org/rfc.html>). IPP es parecido al protocolo web HTTP: tienen la misma cabecera pero distintos datos de uso. Para la comunicación también se utiliza un puerto distinto y específico, el puerto 631, registrado en IANA ((ingl. *Internet Authority for Number Allocation*) o Autoridad en Internet para la Asignación de Nombres).

Los datos se envían al daemon CUPS configurado que suele ser el servidor local. También es posible comunicarse con otros daemons, por ejemplo, con ayuda de la variable shell `CUPS_SERVER`.

Con ayuda de la función de "Broadcast" del daemon CUPS se dan a conocer en la red las impresoras locales que este daemon administra (puerto 631 UDP), apareciendo así en las colas de impresión de todos los daemons que reciban este paquete de broadcast o que puedan leerlo (configurable). Esto supone una ventaja para las redes de empresas ya que de este modo, nada más arrancar el ordenador se pueden *ver* todas las impresoras disponibles sin tener que configurarlas manualmente. Pero esto conlleva un peligro si el ordenador está conectado a Internet. A la hora de configurar la función broadcast debe procurarse que sólo se retransmita en la red local, que el acceso sólo se permita a la red local, y que la dirección IP pública para la conexión a Internet no se encuentre dentro del campo de dirección de la red local. De no ser así, otros usuarios con el mismo proveedor de servicios de Internet también podrían *ver* y utilizar estas impresoras. Además estos broadcasts generan tráfico en la red, lo que implica costes añadidos. Por eso siempre hay que garantizar que tales paquetes de broadcast no sean enviados a Internet por las impresoras locales, p. ej. con ayuda del filtro de paquetes SuSE Firewall (paquete `SuSEfirewall2`). Para recibir el broadcast no es necesario configurar nada más. Sólo al enviar se debe añadir una dirección de broadcast (que p. ej. se puede configurar con `YqST`).

IPP se utiliza para la comunicación entre daemons CUPS locales y remotos (es decir, *servidores CUPS*). Las impresoras de red más modernas también soportan *IPP*. Puede encontrar más información en las páginas web del fabricante o en el manual de la impresora. Asimismo Windows 2000 (y posteriores) ofrece soporte para *IPP*. Lamentablemente surgieron problemas con el formato de implementación, que o han sido resueltos o pueden resolverse con un pack de servicios.

Configuración del servidor CUPS

Existen muchas maneras de configurar impresoras y el daemon con CUPS: a través de la línea de comandos, con `YqST`, el centro del control de KDE, interfaces web, etc. En los siguientes apartados nos centraremos en las herramientas de línea de comandos y en `YqST` pero estas no son ni mucho menos las únicas posibilidades.

Aviso

La interfaz web implica el riesgo de poner en peligro la contraseña del superusuario, ya que ésta se puede enviar a la red en texto sencillo si se da el nombre del ordenador en la URL. Por este motivo, utilice siempre exclusivamente <http://localhost:631/>, y bajo ninguna circunstancia otra dirección.

Aviso

También por esta causa se ha restringido el acceso de administración al daemon CUPS; para que sólo pueda ser configurado cuando la comunicación se realiza mediante "localhost" (lo que es idéntico a la dirección 127.0.0.1) Si se realiza de otra forma, se recibe el correspondiente mensaje de error.

Para administrar impresoras locales es necesario que haya un daemon CUPS en funcionamiento en el ordenador local. Para ello se instala paquete cups y los archivos PPD generados por SuSE en los paquetes paquete cups-drivers y paquete cups-drivers-stp. Después se arranca el servidor (como root) con el comando: `/etc/rc.d/cups restart`. Al configurar con YöST la instalación y el arranque se realizan implícitamente cuando se elige CUPS como sistema de impresión.

PPD, abreviatura de "PostScript Printer Description" o Descripción de Impresoras PostScript, es un estándar para describir opciones de impresión con comandos PostScript. Estos archivos son necesarios en CUPS para la instalación de la impresora. SuSE Linux incorpora archivos PPD generados para diversas impresoras de varios fabricantes. Pero también los fabricantes proporcionan en sus páginas web y CDs de instalación archivos PPD para impresoras PostScript (mayormente en el campo de la "Instalación en Windows NT").

También se puede iniciar el daemon local para hacer que todas las impresoras de todos los servidores de broadcast estén disponibles localmente aunque no exista ninguna impresora local. De esta forma se simplifica en gran medida la selección de impresora en KDE y OpenOffice.

El broadcast se configura con YöST o bien asignando el valor On (por defecto) a la variable "Browsing" en el archivo `/etc/cups/cupsd.conf` y un valor adecuado (por ejemplo 192.168.255.255) a la variable "BrowseAddress". Para que se puedan aceptar trabajos de impresión, se debe permitir la recepción al menos de `<Location /printers>` o mejor incluso `<Location />`. Además debe completarse `Allow From xyz-host.mydomain` – véase <file:///usr/share/doc/packages/cups/sam.html>. Al ejecutar el comando `/etc/rc.d/cups reload` (como root) el daemon acepta la nueva configuración después de haber editado los archivos.

Impresoras de red

Por impresoras de red se entienden normalmente impresoras equipadas con una interfaz de red para un servidor de impresión (como la que ofrece HP con la interfaz JetDirect) o impresoras conectadas a un servidor de impresión o enrutador con la funcionalidad de un servidor de impresión. No nos referimos aquí a ordenadores Windows que ofrecen una impresora compartida o "share"; si bien también se puede establecer comunicación con dichas impresoras fácilmente por medio de CUPS.

La mayor parte de las impresoras de red soportan el protocolo LPD (en el puerto 515). Esto se puede comprobar con el siguiente comando:

```
netcat -z <rechnername>.<domain> 515 && echo ok || echo failed
```

Si este servicio está disponible, se puede configurar con el dispositivo URI (terminología CUPS) `lpd://Server/Queue`. Más sobre los dispositivos URIs en <file:///usr/share/doc/packages/cups/sam.html>.

Suele ser preferible comunicarse con tales impresoras a través del puerto 9100 (HP, Kyocera, etc.) o el puerto 35 (QMS), sin un protocolo LPD conectado de antemano. El nombre del dispositivo URI es entonces:

```
socket://Server:Port/
```

Para imprimir en impresoras Windows, debe estar instalado el paquete `samba-client` y haberse configurado correctamente Samba, el "grupo de trabajo" (workgroup) debe estar bien definido, etc. Los dispositivos URI para ordenadores Windows pueden tener diferentes formas. La más común es: `smb://user:password@host/printer`. Para todas las demás formas posibles, véase <file:///usr/share/doc/packages/cups/sam.html> así como página del manual de `smbpool` (`man smbpool`).

Si ha configurado una impresora de red y posee una pequeña red con varios PCs (Linux), resulta muy útil no tener que configurar las impresoras de red en todos los clientes. Por este motivo debe activarse la funcionalidad "Broadcast" del daemon. Asimismo, no hace falta definir las opciones de configuración como por ejemplo fijar el tamaño estándar del papel a `Letter` en cada uno de los clientes, sino que basta con hacerlo una vez en el servidor. (véase sección [Configuración de la cola de impresión](#) en la página 170). Estas opciones de configuración se almacenan localmente pero aparecen en todos los clientes a través de las herramientas CUPS o el protocolo IPP.

Procesamiento interno de los trabajos

Conversión a PostScript

En principio se puede enviar cualquier tipo de archivo a un daemon CUPS. Los archivos PostScript son los que causan menos problemas. Para realizar una conversión a PostScript a través de CUPS, el tipo de archivo se identifica mediante `/etc/cups/mime.types`, tras lo que se activa la herramienta correspondiente que se encuentra en `/etc/cups/mime.convs`. Esta conversión tiene lugar en el servidor y no en el cliente. Con esto se pretende que las conversiones especiales en las impresoras sólo puedan realizarse en el servidor previsto para esas tareas.

Recuento (ingl. accounting)

Tras la conversión PostScript se averigua el número de páginas del trabajo de impresión. Para ello, CUPS arranca una herramienta (propia) `pstops (/usr/lib/cups/filter/pstops)`. El número de hojas se escribe en `/var/log/cups/page_log`. Las entradas de una línea significan lo siguiente:

- Nombre de impresora (por ejemplo `lp`),
- nombre de usuario (por ejemplo `root`),
- número de trabajo de impresión,
- fecha entre corchetes [],
- página actual del trabajo,
- número de copias,

Filtros de conversión adicionales

También es posible activar otros filtros si se han escogido las opciones correspondientes para la impresión. Los siguientes tienen un interés especial:

psselect si sólo quiere imprimir ciertas hojas del documento,

ps-n-up si quiere imprimir varias páginas del documento en una sola hoja.

Estos filtros no pueden configurarse. En <file:///usr/share/doc/packages/cups/sum.html> se describe cómo activar las opciones.

Conversión específica de impresora

En el siguiente paso se inicia el filtro necesario para generar datos específicos de la impresora. Estos filtros se encuentran en `/usr/lib/cups/filter/`. Qué filtro es el adecuado se indica mediante una entrada `*cupsFilter` en el archivo PPD. Si no existe dicha entrada, se partirá de que se usa una impresora PostScript. En este filtro se definen todas las opciones de impresión que dependen de la impresora, tales como la resolución y el tamaño del papel.

Resulta bastante complicado escribir filtros propios de impresión. Sobre este tema puede consultar el artículo de la base de datos de soporte de SuSE *Using Your Own Filters to Print with CUPS* (palabras clave: "cups" + "filter").

Salida a impresora

Finalmente se activará el backend. Se trata de un filtro especial que envía los datos de impresión a un dispositivo o a una impresora de red (véase `/usr/share/doc/packages/cups/overview.html`). El backend permite la comunicación con el dispositivo o con la impresora de red (depende del dispositivo URI indicado en la instalación). Por ejemplo, si un backend es `usb`, se ejecutará el programa `/usr/lib/cups/backend/usb`. En este punto se abrirá (y bloqueará) el dispositivo USB en el sistema de archivos, se realizará una iniciación preliminar y se enviarán los datos procedentes del filtro. Por último, el dispositivo es iniciado y desbloqueado en el sistema.

Los backends disponibles actualmente son: `paralelo`, `serie`, `usb`, `ipp`, `lpd`, `http`, `socket` (del paquete CUPS) así como `canon` y `epson` (de `cups-drivers-stp`) y `smb` (de `samba-client`).

Sin filtro

Si quiere imprimir sin filtro, indique la opción `-l` en el comando `lpr` o la opción `-oraw` en el comando `lp`. Normalmente la impresión no funciona porque no se realiza ninguna conversión específica de impresora (véase arriba) o no se ponen en funcionamiento otros filtros importantes. Las opciones son similares en otras herramientas CUPS.

Consejos y trucos

OpenOffice

La impresión desde OpenOffice soporta CUPS, de tal manera que no es necesario configurar la impresora como ocurría en StarOffice 5.2. OpenOffice detecta si se está ejecutando un daemon CUPS y solicita a éste las impresoras y opciones disponibles. Una configuración adicional de OpenOffice será innecesaria en un futuro.

Windows

La comunicación con las impresoras de una máquina Windows es posible gracias al dispositivo URI `smb://server/printer` – véase más arriba. En el caso contrario, es decir, si desea imprimir desde Windows en un servidor CUPS, se deben fijar en el archivo de configuración de Samba `/etc/samba/smb.conf` las entradas `printing = CUPS` y `printcap name = CUPS` como corresponde a la preconfiguración en SuSE Linux. Después de modificar `/etc/samba/smb.conf` hay que reiniciar el servidor samba; –véase <file:/usr/share/doc/packages/cups/sam.html>

Configurar impresoras "en crudo" (raw)

Una impresora raw se configura omitiendo en la instalación el archivo PPD, no se realiza ni el filtrado ni el recuento. Para ello los datos deben enviarse en un formato adecuado a la impresora.

Opciones de la impresora

Las opciones de configuración (p. ej. de forma estándar otra resolución) pueden modificarse y guardarse para cada usuario. Estas opciones se almacenan en el archivo `~/ .lpoptions`. Si se elimina del servidor una impresora de este tipo (sin configurar), sigue siendo visible en herramientas como `kprinter` o `xpp`. Se puede seleccionar incluso aunque ya no exista, lo que puede ocasionar problemas. Los usuarios experimentados podrán eliminar las líneas problemáticas de `~/ .lpoptions` con un editor. Véase con este fin el artículo *Print Settings with CUPS* de la base de datos de soporte así como la sección *Configuración de la cola de impresión* en la página 170.

Compatibilidad con LPR

CUPS también puede recibir trabajos de impresión de sistemas LPR. La configuración necesaria en `/etc/xinetd.d/cups - lpd` puede definirse con YaST o bien manualmente.

Búsqueda de errores en CUPS

El archivo de configuración `/etc/cups/cupsd.conf` contiene normalmente la siguiente sección:

```
# LogLevel: controls the number of messages logged to the ErrorLog file
#           and can be one of the following:
#
```

```
#      debug2    Log everything.
#      debug     Log almost everything.
#      info      Log all requests and state changes.
#      warn      Log errors and warnings.
#      error     Log only errors.
#      none      Log nothing.
#
LogLevel info
```

Para buscar errores en CUPS, se define el nivel de depuración o `LogLevel` `debug` y se vuelve a cargar la configuración con `rc cups reload` para que la lea `cupsd`. Una vez hecho esto, encontrará abundantes mensajes en `/var/log/cups/error_log` que le ayudarán a detectar el problema.

Ejecutando antes de una prueba el comando:

```
echo "LABEL $(date)" | tee -a /var/log/cups/error_log
```

se producirá una marca que se transcribirá literalmente en `/var/log/cups/error_log`. De esta forma resultará más fácil encontrar los mensajes después de realizar la prueba.

Imprimir desde aplicaciones

Los programas de aplicación utilizan las colas de impresión disponibles para imprimir desde la línea de comandos. Por lo tanto, en las aplicaciones no es necesario configurar la impresora sino las colas de impresión existentes.

El paquete `cups-client` contiene herramientas de línea de comandos para imprimir con CUPS como p. ej. el comando `lpr`, así que lo dicho anteriormente también funciona con CUPS (ver apartado [Herramientas de línea de comandos para el sistema de impresión CUPS](#) en la página siguiente). No obstante, el diálogo de impresión en los programas de KDE ha de cambiarse en este caso a 'Imprime a través de un programa externo'. De lo contrario no será posible introducir ningún comando de impresión – ver apartado [Configuración rápida de un cliente](#) en la página 184.

Asimismo hay programas gráficos de impresión como `xpp` o el programa de KDE `kprinter` que permiten escoger la cola de impresión y además definir opciones estándar para CUPS y específicas de la impresora del archivo PPD mediante menús gráficos de selección. Para que `kprinter` sea el diálogo de impresión que aparece por defecto en las distintas aplicaciones, introduzca `kprinter`

o `kprinter --stdin` como comando de impresión en la interfaz de impresión de cada aplicación. Cuál de los dos depende de la aplicación en cuestión. De esta forma, tras la interfaz de impresión del programa aparece el diálogo de `kprinter` en el que puede configurar la cola de impresión y otras opciones. Al utilizar este método asegúrese de que las opciones de la interfaz de impresión de la aplicación y de `kprinter` no sean contradictorias. Si es posible, realice la configuración únicamente en `kprinter`.

Herramientas de línea de comandos para el sistema de impresión CUPS

Las herramientas de línea de comandos y las páginas man correspondientes al sistema de impresión CUPS se encuentran en el paquete `cups-client`; la documentación respectiva en el paquete `cups` en `/usr/share/doc/packages/cups/`. En especial cabe destacar el "CUPS Software Users Manual" en <file:///usr/share/doc/packages/cups/sum.html> y el "CUPS Software Administrators Manual" en <file:///usr/share/doc/packages/cups/sam.html>. Ambos están también disponibles localmente en <http://localhost:631/documentation.html> si `cupsd` está ejecutándose en el sistema.

En estas herramientas, el orden de las opciones es importante en algunas ocasiones. Es caso de duda, consulte la página correspondiente del manual.

Para colas de impresión locales

Generar trabajos de impresión

Por lo general se imprime en "System V Art" con `lp -d <cola_impresión> <archivo>` o en "Berkeley Art" con `lpr -P<cola_impresión> <archivo>`.

Puede obtener más información en página del manual de `lpr` (man `lpr`) y página del manual de `lp` (man `lp`) y en la sección "Using the Printing System" unter file:///usr/share/doc/packages/cups/sum.html#USING_SYSTEM del *CUPS Software Users Manual*.

Con el parámetro adicional `-o` es posible fijar opciones suplementarias referentes al tipo de impresión. Puede obtener más información en página del manual de `lpr` (`man lpr`) y página del manual de `lp` (`man lp`) y en la sección "Standard Printer Options" en

[file:/usr/share/doc/packages/cups/sum.html#STANDARD_OPTIONS](file:/usr/share/doc/packages/cups/sum.html#STANDARD_OPTIONS) del *CUPS Software Users Manual*.

Mostrar el estado

El estado de una cola de impresión se muestra en "System V Art" con `lpstat -o <cola_impresión> -p <cola_impresión>` o en "Berkeley Art" con `lpq -P<cola_impresión>`

Sin la indicación de la cola de impresión se mostrarán todas las colas y `lpstat -o` mostrará todos los trabajos de impresión activos con la forma `<cola_impresión>-<número_trabajo>`

Con `lpstat -l -o <cola_impresión> -p <cola_impresión>` se mostrará más información y con `lpstat -t` o bien `lpstat -l -t` se mostrará toda la información disponible.

Puede obtener más información en página del manual de `lpq` (`man lpq`) y página del manual de `lpstat` (`man lpstat`) y en la sección "Using the Printing System" en

[file:/usr/share/doc/packages/cups/sum.html#USING_SYSTEM](file:/usr/share/doc/packages/cups/sum.html#USING_SYSTEM) del *CUPS Software Users Manual*.

Eliminar trabajos de impresión

En "System V Art" con `cancel <cola_impresión>-<número_trabajo>` o en "Berkeley Art" con `lprm -P<cola_impresión> <número_trabajo>` se elimina el trabajo de impresión con el número indicado de la cola especificada. Puede encontrar más información en página del manual de `lprm` (`man lprm`) y página del manual de `cancel` (`man cancel`) y en la sección "Using the Printing System" en

[file:/usr/share/doc/packages/cups/sum.html#USING_SYSTEM](file:/usr/share/doc/packages/cups/sum.html#USING_SYSTEM) del *CUPS Software Users Manual*.

Configuración de la cola de impresión

En la sección "Standard Printer Options" del *CUPS Software Users Manual* que se encuentra en

[file:/usr/share/doc/packages/cups/sum.html#STANDARD_OPTIONS](file:/usr/share/doc/packages/cups/sum.html#STANDARD_OPTIONS) se describen las opciones estándar independientes del hardware para definir el tipo de impresión, y en la sección "Saving Printer Options and Defaults" en

[file:/usr/share/doc/packages/cups/sum.html#SAVING_OPTIONS](file:/usr/share/doc/packages/cups/sum.html#SAVING_OPTIONS)

se describe cómo guardar las distintas opciones.

Las opciones específicas de impresoras para determinar el tipo de impresión se fijan en los archivos PPD que pertenecen a la cola de impresión correspondiente y se muestran de la siguiente manera con el comando

```
lptions -p <cola_impresión> -l:
```

Option/Text: Valor valor valor ...

donde un '*' delante del valor de una opción representa la configuración actual. Ejemplo:

```
PageSize/Page Size: A3 *A4 A5 Legal Letter
Resolution/Resolution: 150 *300 600
```

Aquí la opción `PageSize` está fijada en `A4` y la resolución al valor `300`.

Con `lptions -p <cola_impresión> -o option=valor` se puede configurar otro valor.

Así, en el ejemplo superior, es posible cambiar el tamaño del papel al valor `Letter` en la cola correspondiente con el comando:

```
lptions -p <cola_impresión> -o PageSize=Letter
```

Si un usuario normal ejecuta este comando `lptions`, la configuración sólo se guarda para ese usuario en el archivo `~/lptions`.

Si el administrador del sistema `root` es quien ejecuta el comando `lptions`, las opciones de configuración se convierten en la configuración predeterminada para todos los usuarios del ordenador local y se guardan en el archivo `/etc/cups/lptions`. Los archivos PPD no se modificarán.

Para que los cambios en la configuración sean válidos para todos los usuarios de la red que impriman en una cola de impresión, es necesario modificar la configuración estándar en el archivo PPD de dicha cola. Por ejemplo, el administrador del sistema puede modificar la configuración estándar en el archivo PPD de una cola de impresión de tal forma que el tamaño de papel predeterminado cambie al valor `Letter` en la cola correspondiente para todos los usuarios de la red con:

```
lpadmin -p <cola_impresión> -o PageSize=Letter
```

Véase también el artículo de la SDB (SupportDatabaseArticle) *Print Settings with CUPS*.

Colas de impresión en red

Se sustituye *<servidor_impresión>* por el nombre o la dirección IP del servidor de impresión, y la variable *<cola_impresión>* debe ser una cola que se encuentre en dicho servidor.

Aquí se indican los comandos básicos. Más posibilidades y fuentes de información en la sección *Para colas de impresión locales* en la página 169.

Generar trabajos de impresión

Para generar en "System V Art" un trabajo de impresión en la cola de un servidor de impresión se utiliza

```
lp -d <cola_impresión> -h <servidor_impresión> <archivo>. Como condición previa, el servidor de impresión ha de estar configurado de tal forma que se pueda imprimir en sus colas de impresión. De forma estándar éste no es el caso con CUPS, pero se puede configurar con la configuración de impresoras de Y&ST en una rama de menú avanzado en las opciones de configuración del servidor CUPS.
```

Mostrar el estado

El estado de una cola en un servidor de impresión se muestra en "System V Art" con

```
lpstat -h <servidor_impresión> -o <cola_impresión> -p <cola_impresión>
```

Eliminar trabajos de impresión

Para eliminar un trabajo de impresión de la cola de un servidor de impresión en "System V Art" se utiliza el comando

```
cancel -h <servidor_impresión> <cola_impresión> -<número_trabajo>.
```

Resolución de problemas en CUPS con los comandos anteriores

La resolución de problemas ocurre de forma similar a la descrita en la sección *Resolución de problemas con los comandos anteriores en LPRng* en la página 151, sólo que con CUPS se necesitan otros comandos en el segundo paso:

1. Primero retire todo el papel para que se detenga la impresión.

2. Compruebe con `lpstat -o` (o bien con `lpstat -h <servidor_impresión> -o`) de qué cola es el trabajo que se está imprimiendo y elimínelo con `cancel <cola_impresión>-<número_trabajo>` (o bien con `cancel -h <servidor_impresión> <cola_impresión>-<número_trabajo>`).
3. Si es necesario, utilice el comando `fuser`.
4. Desconecte completamente la impresora.

Acerca de Ghostscript

Ghostscript acepta como entrada datos PostScript y PDF y ofrece numerosos controladores Ghostscript para la conversión a otros formatos. En Ghostscript, estos controladores se denominan "devices".

Ghostscript realiza la conversión en dos pasos:

1. Los datos PostScript son "rasterizados", que el gráfico descrito en PostScript es descompuesto en un raster de píxeles. Este paso se realiza independientemente del controlador Ghostscript empleado. Cuanto más fino es el raster (por tanto cuanto más alta es la resolución), más alta es la calidad de la salida. Hay que tener en cuenta que con una doble resolución, tanto horizontal como verticalmente, se cuadruplica el número de puntos de raster, con lo cual se cuadruplica también el gasto de tiempo de CPU y de memoria.
2. El controlador Ghostscript convierte ahora el gráfico descompuesto en puntos de raster al formato finalmente deseado (p. ej. al lenguaje de impresión deseado).

Ghostscript no se limita a ofrecer controladores de impresoras. También es capaz de procesar archivos PostScript para la salida en pantalla o de convertirlos a PDF. Para visualizar en pantalla archivos PostScript se recomienda utilizar el programa `gv` (paquete `gv`) para visualizar en pantalla archivos PostScript, ya que incorpora una interfaz gráfica para GhostScript.

Ghostscript es un programa muy amplio con múltiples opciones para la línea de comando. La documentación más importante, aparte de página del manual de `gs` (`man gs`) y la lista de los controladores Ghostscript, se encuentra en:

<file:///usr/share/doc/packages/ghostscript/catalog.devices>

así como en los archivos:

```
file:/usr/share/doc/packages/ghostscript/doc/index.html
file:/usr/share/doc/packages/ghostscript/doc/Use.htm
file:/usr/share/doc/packages/ghostscript/doc/Devices.htm
file:/usr/share/doc/packages/ghostscript/doc/hpdj/gs-hpdj.
txt
file:/usr/share/doc/packages/ghostscript/doc/hpijs/hpijs_
readme.html
file:/usr/share/doc/packages/ghostscript/doc/stp/README
```

Después de haber procesado en la línea de comandos la ejecución directa de Ghostscript, se lanza un diálogo con un prompt propio GS> del cual se puede salir con el comando quit.

El comando de ayuda `gs -h` muestra una lista de las opciones más importantes y de los dispositivos soportados. Si se trata de un controlador que tiene soporte para varios modelos, sólo aparece la denominación general del controlador como `uniprint` o `stp`. Los archivos de parámetros para `uniprint` y los modelos de `stp` se incluyen explícitamente en `file:/usr/share/doc/packages/ghostscript/catalog.devices`.

Ejemplos de trabajo con Ghostscript

`file:/usr/share/doc/packages/ghostscript/examples` contiene numerosos archivos de muestra en formato PostScript. La "elipse de color" `file:/usr/share/doc/packages/ghostscript/examples/colorcir.ps` resulta muy adecuada para realizar pruebas de impresión.

Visualización en X11

Para visualizar un archivo de PostScript en X Window System se puede usar el comando `gs`:

```
gs -r600 \
/usr/share/doc/packages/ghostscript/examples/colorcir.ps
```

Con la opción `-r` se especifica la resolución, la cual tiene que ser adecuada para el dispositivo de salida correspondiente (impresora o pantalla) (pruebe p. ej. `-r300`). Para terminar hay que pulsar `(Control) + (C)` dentro de la ventana de terminal desde la que ha ejecutado `gs`.

Conversión a PCL5e

Para convertir un archivo PostScript al formato específico para una impresora PCL5e o PCL6 se usa p. ej. el comando:

```
gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn \
-sDEVICE=ljet4 -r300x300 \
/usr/share/doc/packages/ghostscript/examples/colorcir.ps \
quit.ps
```

El comando debe introducir en una sola línea suprimiendo la barra inversa ('\''), además se supone que el archivo /tmp/out.prn aún no existe.

Conversión a PCL3

Para convertir un archivo PostScript al formato específico para una impresora PCL3 se usa uno de los siguientes comandos:

```
gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn \
-sDEVICE=deskjet -r300x300 \
/usr/share/doc/packages/ghostscript/examples/colorcir.ps \
quit.ps
```

Dependiendo del modelo puede sustituirse el dispositivo *deskjet* por *cdjmomo*, *cdj500* o *cdj550*, o bien utilizar el controlador alternativo *hpdj*:

```
gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn \
-sDEVICE=hpdj -r300x300 \
-sModel=500 -sColorMode=mono -dCompressionMethod=0 \
/usr/share/doc/packages/ghostscript/examples/colorcir.ps \
quit.ps
```

Todos los comandos se han de introducir en *una sola línea* sin '\ '.

Conversión a ESC/P, ESC/P2 o ESC/P-Raster

Para convertir un archivo PostScript al formato específico para una impresora ESC/P2, ESC/P o ESC/P Raster, se usa p. ej. uno de los siguientes comandos:

```
gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn \
@stcany.upp \
/usr/share/doc/packages/ghostscript/examples/colorcir.ps \
quit.ps
```

```
gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn \
-sDEVICE=stcolor -r360x360 \
-dBitsPerPixel=1 -sDithering=gsmono -dnoWeave \
-sOutputCode=plain \
```

```
/usr/share/doc/packages/ghostscript/examples/colorcir.ps \
quit.ps
```

Con estos comandos se ve la diferencia entre el comando de ejecución de Ghostscript usando un archivo de parámetros `stcany.upp` para el controlador `uniprint` y usando otro controlador Ghostscript. Dado que todos los parámetros específicos del controlador se encuentran dentro del archivo de parámetros de `uniprint`, ya no hace falta indicar parámetros específicos, como es el caso en los demás controladores de Ghostscript.

Envío directo a la impresora

Después de ejecutar los comandos arriba indicados, los datos específicos de impresora se encuentran en `/tmp/out.prn`. Suponiendo que la impresora esté conectada al primer puerto paralelo `/dev/lp0`, `root` puede enviar estos datos directamente a la impresora (sin filtro o spooler de impresión) mediante `cat /tmp/out.prn >/dev/lp0`

Procesamiento de PostScript y PDF

Ghostscript puede generar archivos PostScript y PDF, convertir de un formato a otro y enlazar archivos PostScript y PDF entre sí en orden alternante.

Conversión de PostScript a PDF:

```
gs -q -dNOPAUSE -dSAFER \
-sOutputFile=/tmp/colorcir.pdf -sDEVICE=pdfwrite \
/usr/share/doc/packages/ghostscript/examples/colorcir.ps \
quit.ps
```

Conversión del archivo PDF `/tmp/colorcir.pdf` recién creado a PostScript:

```
gs -q -dNOPAUSE -dSAFER \
-sOutputFile=/tmp/colorcir.ps -sDEVICE=pswrite \
/tmp/colorcir.pdf quit.ps
```

Después de reconvertir de PDF a PostScript, el archivo `/tmp/colorcir.ps` ya no coincide con el `/usr/share/doc/packages/ghostscript/examples/colorcir.ps` original. No obstante, en la impresión no debería apreciarse ninguna diferencia.

Enlazar archivos PostScript y PDF a un archivo PostScript:

```
gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.ps \
-sDEVICE=pswrite \
/usr/share/doc/packages/ghostscript/examples/escher.ps \
/tmp/colorcir.pdf quit.ps
```

Enlazar archivos PostScript y PDF a un archivo PDF:

```
gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.pdf \
-sDEVICE=pdfwrite /tmp/out.ps \
/usr/share/doc/packages/ghostscript/examples/golfer.ps \
/tmp/colorcir.pdf quit.ps
```

Desgraciadamente, el enlazar archivos PostScript y PDF entre sí no funciona en todos los casos y depende de los archivos utilizados.

Acerca de a2ps

Para imprimir un archivo de texto ASCII con Ghostscript hay que convertirlo primero a PostScript con el programa `a2ps` (paquete `a2ps`). La conversión es necesaria porque Ghostscript espera PostScript como formato de entrada. Debido a que paquete `a2ps` no está incluido en la instalación estándar, normalmente ha de ser instalado manualmente. `a2ps` es una herramienta muy potente para convertir texto plano a un formato PostScript de calidad. `a2ps` es un programa muy completo y dispone de múltiples opciones para la línea de comandos. La documentación más importante se encuentra en página del manual de `a2ps` (`man a2ps`) – la documentación completa está disponible en la página de información de `a2ps`.

Impresión directa de un archivo de texto con a2ps

Para convertir un archivo de texto a PostScript con `a2ps` de tal forma que se impriman 2 páginas de tamaño reducido en una sola hoja, se puede usar el siguiente comando:

```
a2ps -2 ---medium=A4dj ---output=/tmp/out.ps archivo_texto
```

Para controlar la salida de `a2ps` puede ejecutar

```
gs -r60 /tmp/out.ps
```

pudiendo así visualizar en la pantalla el archivo PostScript generado. Puede pasar a la página siguiente del documento pulsando return en la ventana de terminal desde la que ha ejecutado el comando `gs` (`(Control) + C`) para terminar).

La salida de `a2ps` puede convertirse al formato específico de impresora con

```
gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn \
(driver-parameter) /tmp/out.ps quit.ps
```

Aquí es necesario introducir un parámetro *<driver-parameter>* adecuado para la impresora tal y como se ha visto en el apartado anterior.

La salida de Ghostscript puede enviarse a la impresora directamente (es decir, sin spooler ni filtro de impresión) como `root` con

```
cat /tmp/out.prn >/dev/lp0
```

siempre y cuando la impresora esté conectada al primer puerto paralelo `/dev/lp0`.

Reformatear PostScript con `psutils`

Para reformatear es necesario en primer lugar imprimir en un archivo `/tmp/in.ps` desde una aplicación y comprobar con `file /tmp/in.ps` que se ha creado realmente un archivo PostScript.

El paquete `psutils` contiene diversos programas para reformatear datos PostScript. En especial el programa `pstops` permite llevar a cabo cambios de gran alcance. Véase la página del manual de `pstops` (`man pstops`). Puesto que el paquete `psutils` no está instalado de forma estándar, deberá instalarse manualmente.

Los siguientes comandos sólo funcionan para archivos PostScript que han sido "tan bien" generados que es posible reformatearlos. Aunque éste suele ser el caso normal, dependiendo de la aplicación que ha generado el archivo PostScript puede resultar imposible.

psnup

Con `psnup -2 /tmp/in.ps /tmp/out.ps` se convierte `/tmp/in.ps` a `/tmp/out.ps`, con lo que se representarán dos páginas reducidas en una sola hoja. Puesto que la complejidad de la impresión por página se incrementa al reducir dos páginas en una hoja, algunas impresoras PostScript que no dispongan de memoria suficiente pueden no funcionar correctamente.

pstops

Se puede fijar un tamaño y posición individual con `pstops` de la forma siguiente:

```
pstops '1:0@0.8(2cm,3cm)' /tmp/in.ps /tmp/out.ps
```

Aquí se escala con el factor 0.8, con lo que una página A4 de aproximadamente 21x30 cm se reduce a aprox. 17x24 cm. Eso provoca que haya un margen adicional a la derecha de unos 4 cm y en la parte superior de 6 cm. Además todo se desplaza 2 cm a la derecha y 3 cm hacia arriba para que los márgenes tengan el mismo grosor en toda la página.

Este comando `pstops` ofrece un nivel muy alto de reducción y utiliza márgenes muy generosos a fin de que también funcione en aplicaciones que tengan nociones un tanto optimistas de lo que debe caber en una página. Con esto nos referimos a aquellas en las que la impresión de la aplicación en `/tmp/in.ps` es en realidad demasiado grande.

Un ejemplo adicional

```
pstops '1:0@0.8(2cm,3cm)' /tmp/in.ps /tmp/out1.ps
psnup -2 /tmp/out1.ps /tmp/out.ps
```

Con estos comandos se consigue que quepan dos páginas reducidas en una sola hoja, pero con mucho espacio entre ambas páginas reducidas. Es mejor posicionar individualmente cada página:

```
pstops '2:0L@0.6(20cm,2cm)+1L@0.6(20cm,15cm)' \
/tmp/in.ps /tmp/out.ps
```

El comando debe introducirse en una sola línea sin barra inversa `'\'`.

Sobre el efecto de

```
pstops '2:0L@0.6(20cm,2cm)+1L@0.6(20cm,15cm)':
```

2:0 ... +1 significa que dos páginas se sitúan la una al lado de la otra, donde las páginas módulo 2 se cuenta de manera alternativa como página 0 (módulo 2) y página 1 (módulo 2).

0L@0.6(20cm,2cm) significa que la página 0 (módulo 2) respectiva se gira 90 grados a la izquierda, se escala con el factor 0.6 y se mueve 20 cm hacia la derecha y 2 cm hacia arriba

1L@0.6(20cm,15cm) de forma análoga se gira la página 1 (módulo 2) correspondiente 90 grados, se escala con el factor 0.6 y se mueve 20 cm hacia la derecha y 15 cm hacia arriba.

En PostScript el punto cero del sistema de coordenadas es la esquina inferior izquierda de la hoja de papel, aquí indicado con `+` (ver Fig. *pstops* en la página siguiente):

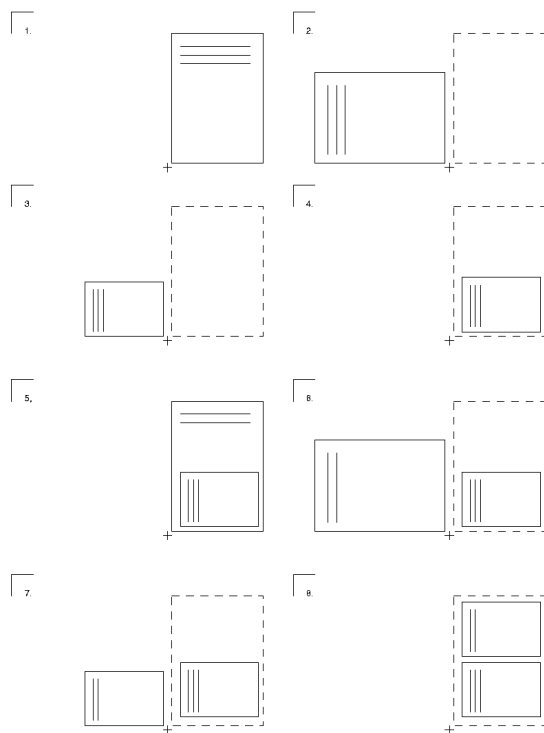


Figura 6.2: Ejemplificación de los pasos con *pstops*

1. Aquí una página 0 (módulo 2) con tres líneas de texto:
2. Después de un giro a la izquierda de 90 grados:
3. Después de escalar con el factor 0.6:
4. Después de mover 20 cm a la derecha y 2 cm hacia arriba:
5. Encima se coloca una página 1 (módulo 2) con dos líneas de texto:
6. Tras girar la página 1 (módulo 2) a la izquierda 90 grados:
7. Después de escalar la página 1 (módulo 2) con el factor 0.6:
8. Después de mover la página 1 (módulo 2) 20 cm a la derecha y 15 cm hacia arriba:

psselect

Con `psselect` se pueden seleccionar páginas sueltas. Con el comando `psselect -p2-5 /tmp/in.ps /tmp/out.ps` se seleccionan las páginas 2, 3, 4 y 5 de `/tmp/in.ps` y se mandan a `/tmp/out.ps`. Con `psselect -p-3 /tmp/in.ps /tmp/out.ps` se seleccionan todas las páginas hasta la página 3. El comando `psselect -r -p4- /tmp/in.ps /tmp/out.ps` selecciona desde la página 4 hasta el final y las imprime en orden inverso.

Control en la pantalla con Ghostscript

Se puede mostrar el archivo PostScript `/tmp/out.ps` página por página en la interfaz gráfica de Ghostscript con `gs -r60 /tmp/out.ps` pulsando la tecla Enter en la ventana de terminal en la que se ha ejecutado Ghostscript. Para finalizar pulse las teclas `(Control) + (C)`.

El programa `gv` del paquete `gv` es un frontal gráfico para Ghostscript. Se activa desde la interfaz gráfica con `gv /tmp/out.ps` y permite la representación apropiada de formatos apaisados, ampliaciones o reducciones de la representación (pero no del archivo PostScript en sí) y la selección de páginas sueltas (por ejemplo para imprimir las directamente desde `gv`).

Codificación de texto ASCII

En texto plano cada carácter se guarda codificado como un determinado número. El símbolo visual que corresponde al carácter codificado está determinado en tablas de código. Dependiendo de la tabla de código usada por un programa o filtro de impresión, la visualización del mismo código en la pantalla y en la impresora puede variar.

Las combinaciones estándar de caracteres son códigos numéricos de 0 a 255. Los caracteres con los códigos 0 a 127 son los llamados caracteres ASCII, que incluyen las letras "normales", cifras y signos especiales (aunque sin los caracteres específicos de un país) y siempre se determinan de la misma forma.

Los códigos 128 a 255 se utilizan para los caracteres específicos de un país (p. ej. los acentos). Puesto que de hecho hay más de 128 caracteres específicos de país, los códigos 128 a 255 no se ocupan siempre de la misma forma, sino que dependiendo del país, un mismo código es utilizado para signos distintos.

ISO-8859-1 (también *Latín 1*) es la codificación usada para idiomas de Europa Occidental e ISO-8859-2 (también *Latín 2*) se usa para codificar los

idiomas de Europa del Este y Central. Así p. ej., el código 241 (octal) significa, según ISO-8859-1, el signo de abrir exclamación, mientras que en ISO-8859-2 representa una A con Ogonek. ISO-8859-15 equivale en lo esencial a ISO-8859-1, si bien en él código 244 (octal) representa al símbolo del Euro.

Ilustración

Todos los comandos deben introducirse en una sola línea suprimiendo la barra inversa ('\'') al *final de línea*.

Genere un archivo ejemplo de texto ASCII con:

```
echo -en "\rCode 241(octal): \
\241\r\nCode 244(octal): \244\r\f" >example
```

Visualización en pantalla

Abra tres ventanas de terminal en el entorno gráfico mediante los comandos:

```
xterm -fn *-***-14-***-iso8859-1 -title iso8859-1 &
xterm -fn *-***-14-***-iso8859-15 -title iso8859-15 &
xterm -fn *-***-14-***-iso8859-2 -title iso8859-2 &
```

Puede visualizar el archivo ejemplo en cada una de ellas con el comando `cat example`.

En "iso8859-1" se ve:

código 241 como signo de abrir exclamación (castellano)

código 244 como círculo con ganchillo (signo común de moneda)

En "iso8859-15" se ve:

código 241 como signo de abrir exclamación (castellano)

código 244 como signo de Euro

En "iso8859-2" se ve:

código 241 como A mayúscula con ganchillo (A con Ogonek)

código 244 como círculo con ganchillo (signo común de moneda)

Debido a la codificación establecida no es posible utilizar simultáneamente diversos caracteres específicos de países. Así p. ej. el símbolo del Euro no se puede representar en el mismo texto junto con una A con Ogonek.

Más información en la visualización correcta respectivamente: En "iso8859-1": página del manual de `iso_8859-1` (`man iso_8859-1`). En "iso8859-2": página del manual de `iso_8859-2` (`man iso_8859-2`). En "iso8859-15": página del manual de `iso_8859-15` (`man iso_8859-15`).

Salida impresa

Dependiendo de la codificación establecida para la correspondiente cola de impresión, la salida impresa del texto ASCII (p. ej. el resultado impreso del archivo `example`) será análoga a estos casos. La salida impresa de documentos generados con sistemas de tratamiento de textos no suele depender de la codificación, ya que el formato de salida de impresión de dichos sistemas es PostScript y no texto ASCII.

Al imprimir el archivo `example`, la salida impresa presenta la codificación utilizada en el sistema de impresión para texto ASCII. `a2ps` permite convertir el archivo `example` a PostScript y así establecer la codificación individualmente:

```
a2ps -1 -X ISO-8859-1 -o example-ISO-8859-1.ps example
a2ps -1 -X ISO-8859-15 -o example-ISO-8859-15.ps example
a2ps -1 -X ISO-8859-2 -o example-ISO-8859-2.ps example
```

Al imprimir los archivos PostScript `example-ISO-8859-1.ps`, `example-ISO-8859-15.ps` y `example-ISO-8859-2.ps`, la salida impresa presenta la codificación establecida con `a2ps`.

Impresión en redes TCP/IP

Puede encontrar información más detallada sobre el spooler LPRng en *LPRng-Howto* en

<file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html>. Respecto a CUPS, véase *CUPS Software Administrators Manual* en <file:/usr/share/doc/packages/cups/sam.html>

Aclaración de términos

Servidor de impresión Por *servidor de impresión* se entiende aquí un ordenador completo con tiempo de CPU y capacidad de memoria suficientes.

Printserver-Box o impresora de red

- Un servidor de impresión dedicado (printserver-box) es un pequeño dispositivo con conexión a la red TCP/IP y posibilidad de conexión local para una impresora. También existen las llamadas *router boxes* que cuentan con una posibilidad de conexión para una impresora y se manejan igual que las impresoras de red.

- Una impresora de red tiene una conexión propia a la red TCP/IP y es en última instancia una impresora que incorpora un servidor de impresión dedicado. Se trabaja de la misma forma con servidores de impresión dedicados que con impresoras de red.

Existe una diferencia importante entre una impresora de red o un servidor de impresión dedicado por un lado y un verdadero servidor de impresión por el otro. Asimismo hay impresoras grandes con las que se suministra un ordenador que hace las funciones de servidor de impresión para imprimir en la red. Pero en este caso, los trabajos de impresión no se envían a la impresora, sino al servidor de impresión incluido.

Servidor LPD Ein *LPD-Server* ist ein Print-Server, der über das LPD-Protokoll ansprechbar ist. Das ist der Fall, wenn auf dem Print-Server das *LPRng/lpdfilter* Drucksystem (genaugenommen der *lpd*) läuft oder wenn das *CUPS* Drucksystem läuft und dieses so konfiguriert wurde, dass der Rechner auch über das LPD-Protokoll ansprechbar ist (genaugenommen über den *cups-lpd*).

Servidor IPP o servidor CUPS Un *servidor IPP* o *servidor CUPS* es un servidor de impresión al que puede accederse por medio del protocolo IPP. Éste es el caso cuando en el servidor de impresión funciona el sistema de impresión CUPS (o más exactamente *cupsd*).

Servidor de red CUPS Denominamos *servidor de red CUPS* a un *servidor CUPS* configurado de tal forma que comunique vía broadcast UDP (a través del puerto UDP 631) sus colas de impresión a otros ordenadores en la red.

Configuración rápida de un cliente

Generalmente, un cliente en la red no dispone de una impresora conectada localmente, sino que los trabajos de impresión son enviados por el cliente a un servidor de impresión. En caso de tener un servidor de impresión además de una impresora conectada localmente al cliente, deberá configurar no sólo el cliente sino también la impresora conectada localmente. En el cliente se ha de seleccionar un sistema de impresión adecuado al que existe en el servidor de impresión.

Configuración de cliente para un servidor LPD

Si en la red no existe ningún servidor de red CUPS sino tan sólo un servidor LPD, debe utilizar el sistema de impresión *LPRng/lpdfilter* en el cliente. No es necesario configurar el cliente de manera adicional, ya que con el spooler

LPRng se puede acceder directamente a colas de impresión remotas con el comando `lpr`. Véase la sección *Herramientas de línea de comandos para LPRng* en la página 147.

El único requisito es que el servidor LPD esté configurado de forma que el cliente pueda imprimir en su cola de impresión. Para imprimir desde aplicaciones, introduzca como comando de impresión

```
lpr -P<cola_impresión>@<servidor_impresión>
```

, es decir, como en el apartado *Para colas de impresión remotas* en la página 150 pero sin especificar ningún archivo.

Algunos programas están ya preconfigurados para CUPS y su configuración ha de modificarse para LPRng. Especialmente en el caso de KDE y su programa de impresión `kprinter` ha de seleccionarse la opción 'Imprime a través de un programa externo'. En caso contrario no será posible introducir el comando de impresión mencionado arriba.

Configuración de cliente para un servidor de red CUPS

Si el servidor de impresión es un servidor de red CUPS, puede elegir entre las siguientes posibilidades al seleccionar 'Editar' y 'Avanzada' en la configuración de impresora de YaST:

CUPS como servidor (por defecto en la instalación estándar) Si no existe ninguna impresora conectada localmente, no se ha configurado ninguna cola local con YaST. En este caso, `cupsd` no se inicia automáticamente. Para iniciar `cupsd` tiene que activar el servicio 'cups' (normalmente para los niveles de ejecución 3 und 5).

No es necesario configurar el cliente de manera adicional, ya que un servidor de red CUPS comunica periódicamente sus colas a todos los ordenadores de la red por medio de un broadcast. De esta forma, las colas del servidor de red CUPS estarán disponibles automáticamente en el cliente en muy poco tiempo.

Como único requisito, el servidor de red CUPS ha de estar configurado de tal forma que la función de broadcast esté activada, que se utilice una dirección broadcast adecuada para el cliente y que el cliente esté autorizado a imprimir en las colas del servidor de red CUPS.

CUPS exclusivamente como cliente Para imprimir en las colas de impresión del servidor de red CUPS, es suficiente con que CUPS funcione sólo como cliente. Para ello basta con introducir el nombre del servidor de red CUPS en la configuración de impresión *Client-only* de YaST.

En este caso, en el cliente no funciona ningún cupsd y no existe por tanto el archivo `/etc/printcap`. Sin embargo, los programas que no son compatibles con CUPS ofrecen sólo las colas incluidas en el archivo `/etc/printcap` local. En este caso se recomienda que, cuando CUPS funcione como servidor, el cupsd local cree automáticamente un archivo `/etc/printcap` con el nombre de las colas del servidor de red CUPS.

Protocolos para imprimir en una red TCP/IP

Existen distintas posibilidades de impresión en una red TCP/IP, las cuales no dependen tanto del hardware como del protocolo utilizado. Por eso en la configuración con YvST se distingue en función del protocolo y no del hardware. No obstante, en la configuración de impresora en YvST primero hay que seleccionar con qué tipo de "hardware" se va a imprimir (p. ej. a través de un servidor de red CUPS, un servidor de red LPD o directamente en una impresora de red o servidor de impresión dedicado). Según la opción escogida se ofrecen los protocolos posibles; si bien el protocolo que debería funcionar en la mayoría de los casos está preseleccionado. Si sólo un protocolo es posible, no se ofrece ninguna selección.

- Imprimir a través de un servidor de red CUPS
 - Protocolo IPP (única posibilidad)
- Imprimir a través de un servidor de red LPD
 - Protocolo LPD (única posibilidad)
- Imprimir directamente desde una impresora de red o servidor de impresión dedicado:
 - Socket TCP
 - Protocolo LPD
 - Protocolo IPP

Para poder transmitir datos del remitente al destinatario según un protocolo determinado, es necesario que ambos soporten dicho protocolo. El software que funciona en el remitente y el destinatario también debe soportar ese protocolo. Por consiguiente, el hardware y el software empleados no son relevantes: lo importante es que tanto el remitente como el destinatario soporten el protocolo correspondiente. Dependiendo del protocolo utilizado, se transmiten trabajos de impresión o sólo datos en crudo.

Además de los datos que se van a imprimir, un trabajo de impresión contiene también datos adicionales — qué usuario ha creado el trabajo de impresión y en qué máquina o, en caso necesario, opciones específicas de impresión (p. ej. tamaño del papel, impresión en modo dúplex, etc.).

Imprimir a través del protocolo LPD

En este caso, el remitente envía la tarea de impresión a través del protocolo LPD a una cola de impresión en el destinatario. Según el protocolo LPD, el destinatario recibe los trabajos de impresión en el puerto 515. Por lo tanto, en el ordenador destinatario siempre se requiere un servicio que acepte los trabajos de impresión en el puerto 515 (este servicio se llama normalmente lpd). Asimismo, también se requiere una cola de impresión a la que mandar los trabajos aceptados.

Remitentes que soportan el protocolo LPD

Ordenadores Linux con el sistema de impresión LPRng:

- LPRng soporta el protocolo LPD mediante lpd. Para ello se necesita una cola de impresión local mediante la cual el lpd del remitente reenvía el trabajo de impresión al lpd del destinatario.
- Con LPRng la transmisión se puede hacer también sin lpd local. El programa lpr del paquete lprng puede reenviar la tarea de impresión directamente al lpd del destinatario utilizando el protocolo LPD.

Ordenadores Linux con el sistema de impresión CUPS (servidor):

- CUPS soporta el protocolo LPD sólo a través del daemon cupsd. Para ello se necesita una cola de impresión local mediante la cual el cupsd local reenvía la tarea de impresión al lpd del destinatario.

Ordenadores Linux con el sistema de impresión CUPS (cliente):

- La transmisión de datos a través del protocolo LPD no está soportada en los clientes CUPS.

Otros sistemas operativos:

- El protocolo LPD es muy antiguo, por lo que cualquier sistema operativo debería soportarlo al menos como remitente. Es posible que no se soporte por defecto. En este caso habría que instalar manualmente el software necesario.

Destinatarios que soportan el protocolo LPD

Ordenadores Linux con el sistema de impresión LPRng:

- LPRng soporta la recepción de datos a través del protocolo LPD mediante lpd.

Ordenadores Linux con el sistema de impresión CUPS (servidor):

- CUPS soporta la recepción de datos a través del protocolo LPD mediante cups-lpd. Puede activar cups-lpd por medio de inetd o xinetd.

Ordenadores Linux con el sistema de impresión CUPS (cliente):

- Los clientes CUPS no soportan la recepción de datos a través del protocolo LPD.

Servidor de impresión e impresora de red/servidor de impresión dedicado

- El protocolo LPD es muy antiguo, por lo que cualquier servidor de impresión, servidor de impresión dedicado o impresora de red de uso extendido debería soportar este protocolo.
- En los servidores de impresión dedicados e impresoras de red el nombre de las colas de impresión varía en función del modelo o existen varias colas de impresión que funcionan de forma distinta.

Imprimir a través del protocolo IPP

Aquí el remitente envía la tarea de impresión a través del protocolo IPP a una cola de impresión en el destinatario. Según el protocolo IPP, el remitente acepta los trabajos de impresión en el puerto 631. Por lo tanto, en el ordenador destinatario se requiere un servicio que acepte los trabajos de impresión en el puerto 631 (este servicio se llama en CUPS cupsd) y una cola de impresión en la que se guarden los trabajos aceptados.

Remitentes que soportan el protocolo IPP:

Ordenadores Linux con el sistema de impresión LPRng:

- LPRng no soporta el protocolo IPP.

Ordenadores Linux con CUPS como cliente o servidor

- CUPS también soporta el envío de datos a través del protocolo IPP sin cupsd local. Los programas lpr o lp del paquete cups-client o el programa xpp o el programa KDE kprinter pueden reenviar el trabajo de impresión a través del protocolo IPP directamente al destinatario.

Otros sistemas operativos:

- El protocolo IPP es relativamente nuevo, por lo que el soporte depende de cada caso concreto.

Destinatarios que soportan el protocolo IPP

Ordenadores Linux con el sistema de impresión LPRng:

- LPRng no soporta el protocolo IPP.

Ordenadores Linux con el sistema de impresión CUPS (servidor):

- CUPS soporta la recepción a través del protocolo IPP mediante cupsd. En el ordenador destinatario se requiere una cola de impresión en la que cups-lpd guarde el trabajo de impresión que ha recibido del remitente.

Ordenadores Linux con el sistema de impresión CUPS (cliente):

- Los clientes CUPS no soportan la recepción a través del protocolo IPP.

Servidor de impresión e impresora de red/servidor de impresión dedicado

- El protocolo IPP es relativamente nuevo, por lo que el soporte depende de cada caso concreto.

Imprimir directamente vía socket TCP

Aquí no se envía ninguna tarea de impresión a una cola de impresión remota, ya que no existe ningún protocolo (LPD o IPP) que pueda trabajar tanto con trabajos como con colas de impresión. En vez de esto se envían directamente datos en crudo a un puerto TCP remoto utilizando el socket TCP. Normalmente se utiliza para enviar datos específicos de una impresora a impresoras de red y servidores de impresión dedicados. En muchos casos se emplea el puerto TCP 9100.

Remitentes que soportan la impresión directa a través del socket TCP:**Ordenadores Linux con el sistema de impresión LPRng:**

- LPRng soporta el envío directo a través del socket TCP mediante lpd. Se requiere una cola en el ordenador remitente de la que el lpd del remitente tome el trabajo de impresión y envíe los datos que se van a imprimir al puerto TCP del destinatario.
- LPRng también lo soporta sin lpd local. El programa lpr del paquete lprng puede enviar directamente los datos al puerto TCP del destinatario a través del socket TCP con la opción -Y. Véase al respecto la página del manual correspondiente a lpr.

Ordenadores Linux con el sistema de impresión CUPS (servidor):

- CUPS soporta el envío directo de datos a través del socket TCP por medio de cupsd. Se requiere una cola en el ordenador remitente desde la que cupsd tome el trabajo de impresión y envíe los datos que se van a imprimir al puerto TCP del destinatario.

Ordenadores Linux con el sistema de impresión CUPS (cliente):

- Los clientes CUPS no soportan el envío directo a través del socket TCP.
- No obstante, los siguientes comandos permiten enviar datos al puerto de un ordenador.

```
cat <archivo> | netcat -w 1 <host> <puerto>
```

Destinatarios que soportan la impresión directa a través del socket TCP:

Ordenadores Linux con LPRng o con CUPS como cliente o servidor

- Para la recepción directa a través del socket TCP no se requiere ningún sistema de impresión y ningún sistema de impresión lo soporta directamente, ya que normalmente no tiene sentido enviar datos en crudo cuando existe un sistema de impresión que soporta trabajos de impresión con sus protocolos correspondientes (LPD o IPP).
- No obstante, p. ej. en el sistema de impresión CUPS es posible aceptar datos en el puerto 9100 y reenviarlos a una cola de impresión. Para ello debe introducirse en `/etc/inetd.conf` alguna de las líneas siguientes:

```
9100 stream tcp nowait lp /usr/bin/lp lp -d  
<cola_impresión>
```

Si no se va a realizar ningún proceso de filtrado, añada `-o raw`.

- También es posible emular un servidor de impresión dedicado que recibe datos en el puerto 9100 y los envía directamente a la impresora. Para ello debe introducirse en `/etc/inetd.conf` una línea del tipo:

```
9100 stream tcp nowait lp /bin/dd dd of=/dev/lp0
```

Impresora de red o servidor de impresión dedicado

- El soporte depende de cada caso concreto.
- Especialmente el puerto correcto varía en función del modelo. Con impresoras de red HP o servidores de impresión dedicados HP JetDirect, este suele ser el puerto 9100, o con servidores de impresión dedicados JetDirect con dos o tres conexiones para impresoras suele ser los puertos 9100, 9101 y 9102. Estos puertos también son utilizados por muchos otros servidores de impresión dedicados. Consulte el manual de servidores de impresión dedicados y, en caso de duda, pregunte al fabricante del servidor o de la impresora de red qué puerto utiliza la impresora

para comunicarse. Puede encontrar más información en LPRng-Howto en

```
file:///usr/share/doc/packages/lprng/
LPRng-HOWTO.html
```

y allí más concretamente en

```
file:///usr/share/doc/packages/lprng/
LPRng-HOWTO.html#SECNETWORK,
file:///usr/share/doc/packages/lprng/
LPRng-HOWTO.html#SOCKETAPI
file:///usr/share/doc/packages/lprng/
LPRng-HOWTO.html#AEN4858
```

Ejemplos

Caso 1: Varias estaciones de trabajo, un servidor de impresión y uno o varios servidores de impresión dedicados o impresoras de red:

Servidor de impresión con LPRng

- Las estaciones de trabajo han de utilizar también el sistema de impresión LPRng.
- En el servidor de impresión existe una cola para cada impresora conectada al servidor de impresión dedicado o para cada impresora de red.
- Las estaciones de trabajo transmiten los trabajos de impresión a través del protocolo LPD a la cola de la impresora en el servidor de impresión.
- Dependiendo del protocolo soportado por el servidor de impresión dedicado o la impresora de red, el servidor de impresión utiliza el protocolo LPD o la transmisión directa de datos a través del socket TCP para enviar los datos al servidor de impresión dedicado/impresora de red.

Servidor de impresión con CUPS como servidor

- Las estaciones de trabajo han de utilizar también el sistema de impresión CUPS. El sistema CUPS como cliente es más que suficiente en este caso.
- En el servidor de impresión existe una cola para cada impresora conectada al servidor de impresión dedicado o para cada impresora de red.
- Las estaciones de trabajo transmiten los trabajos de impresión a través del protocolo IPP a la cola de la impresora en el servidor de impresión.

- Dependiendo del protocolo soportado por el servidor de impresión dedicado o la impresora de red, el servidor de impresión utiliza el protocolo LPD o la transmisión directa de datos a través del socket TCP para enviar los datos al servidor de impresión dedicado/impresora de red.

Caso 2: Unas pocas estaciones de trabajo, ningún servidor de impresión y una o varias impresoras de red o servidores de impresión dedicados.

Estaciones de trabajo con LPRng o CUPS como servidor

- En cada estación de trabajo existe una cola para cada impresora conectada al servidor de impresión dedicado o para cada impresora de red. Debido a que es necesario configurar todas las colas en cada estación de trabajo, este escenario sólo se recomienda en caso de tener pocas estaciones de trabajo.
- Dependiendo del protocolo soportado por el servidor de impresión dedicado o impresora de red, las estaciones de trabajo utilizan el protocolo LPD o la transmisión directa de datos a través del socket TCP para enviar los datos al servidor de impresión dedicado o a la impresora de red.
- En caso de que varias estaciones de trabajo envíen simultáneamente datos a la misma impresora de red o servidor de impresión dedicado, pueden producirse problemas incluyendo la pérdida de datos, sobre todo si se ha empleado el protocolo LDP para transmitir los datos. El motivo es que la implementación del destinatario LPD en la impresora de red o servidor de impresión dedicado suele ser deficiente por falta de memoria suficiente para aceptar y guardar temporalmente varios trabajos de impresión. En cambio, la transmisión de datos a través del socket TCP suele resultar muy fiable.

Filtros en la impresión en red

En el apartado anterior se ha explicado cómo se transmiten trabajos de impresión o datos en crudo de la estación de trabajo a la impresora. Ahora veremos cómo se realiza el proceso de filtrado (la transformación de los datos originales en datos específicos de la impresora) al imprimir en red. El filtrado en la red se produce de la misma forma que en una impresora conectada a un ordenador autónomo y los filtros de impresión son también los mismos. La única diferencia

radica en que el flujo de datos de la estación de trabajo a la impresora sigue un camino más complicado y pasa por varias estaciones; p. ej.:

Estación de trabajo → servidor de impresión → printserver-box → impresora

Es en esta posición donde el archivo de salida se convierte al formato que puede imprimir la impresora (PostScript, PCL, ESC/P).

La conversión se realiza por medio de filtros de impresión que sólo funcionan en un ordenador que tenga la cantidad de memoria y el rendimiento necesarios. Es decir, en una estación de trabajo o un servidor de impresión pero no en una impresora de red ni en el servidor de impresión dedicado. Estos últimos no suelen incluir ningún filtro de impresión, sólo pueden aceptar datos específicos de impresora y enviarlos a la impresora.

Una cola de impresión puede crearse con o sin filtrado. En la configuración de impresora en YoST hay que seleccionar primero el "hardware" (p. ej. a través del servidor de red CUPS, servidor de red LPD o impresión directa a una impresora de red o servidor de impresión dedicado) sobre el que se va a imprimir. Por este motivo, la configuración predeterminada referente a la existencia de filtrado suele ser la más adecuada para el proceso de impresión. Si es necesario, las opciones de configuración estándar pueden modificarse.

Las opciones de configuración predeterminadas son:

Imprimir a través de un servidor de red CUPS sin filtrado (ya que el filtrado se produce normalmente en el servidor de red CUPS).

Imprimir a través de un servidor de red LPD sin filtrado (ya que el filtrado se produce normalmente en el servidor de red LDP).

Imprimir directamente a una impresora de red o servidor de impresión dedicado: filtrado

Al crear la cola con filtrado, los datos originales se guardan temporalmente en la cola. Cuando estos datos se envían al destinatario, pasan por el filtro que se encuentra en el ordenador que contiene la cola. El filtrado se lleva a cabo antes de enviar los datos para que el destinatario los reciba ya reformateados (figura [Filtros en la impresión en red](#) en la página siguiente).

A continuación se muestran las posibilidades de filtrado en los ejemplos superiores:

Caso B1: Varias estaciones de trabajo, un servidor de impresión y uno o varios servidores de impresión dedicados o impresoras de red:

La configuración más sencilla y útil es la que se ilustra en la figura [Filtros en la impresión en red](#) en la página 195.

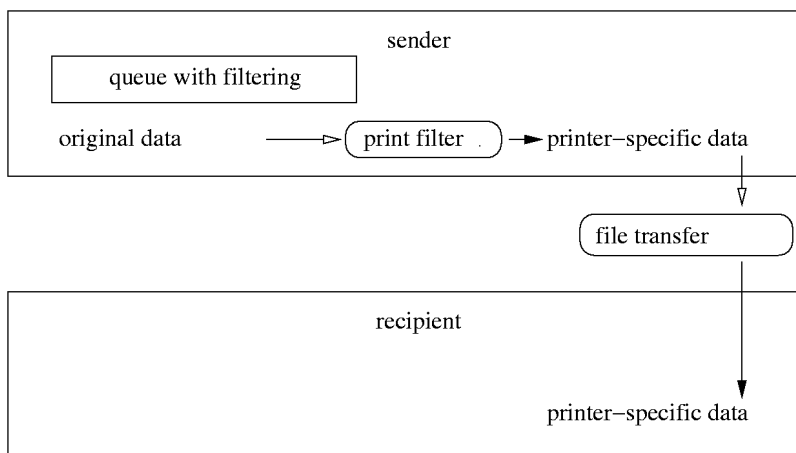


Figura 6.3: Resumen del proceso de filtrado

Caso B1b Para cada cola con filtrado en el servidor de impresión puede configurarse una cola sin filtrado en cada estación de trabajo para que, en caso de fallo o sobrecarga en el servidor de impresión, los datos puedan almacenarse temporalmente en las estaciones de trabajo y se pueda imprimir hasta que el servidor vuelva a estar disponible. La desventaja es que hay que configurar todas las colas de impresión en cada una de las estaciones de trabajo (sin filtro) y en caso de cambiar las colas en el servidor, la configuración ha de cambiarse también en las estaciones de trabajo.

La figura *Filtros en la impresión en red* en la página 196 muestra esta configuración algo más compleja:

Caso B1c En teoría, el filtrado podría producirse en las estaciones de trabajo y el servidor de impresión se limitaría a transmitir los datos específicos de impresora a la impresora de red o servidor de impresión dedicado. Esto sólo tiene sentido si el servidor de impresión tiene tan poca potencia que el proceso de filtrado ocasiona una sobrecarga. Los inconvenientes son que habría que configurar (con filtro) las colas en todas las estaciones de trabajo y en caso de cambiar la configuración de las colas, ésta habría de cambiarse también en todas las estaciones de trabajo.

Esta configuración es la que se muestra en la figura *Filtros en la impresión en red* en la página 197.

Caso B2 Unas pocas estaciones de trabajo, ningún servidor de impresión y una

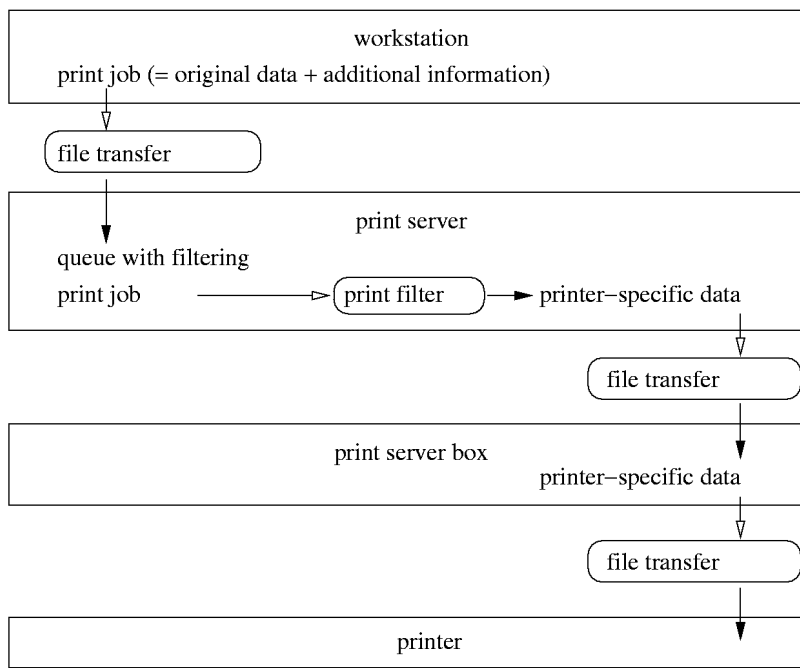


Figura 6.4: Configuración 1

o varias impresoras de red o servidores de impresión dedicados.

La única configuración posible sería tener en cada estación de trabajo una cola con filtro para cada impresora. El inconveniente es que habría que configurar las colas en todas las estaciones de trabajo (con filtro) y en caso de cambiar la configuración, habría que adaptar también la configuración en todas las estaciones de trabajo.

La configuración se refleja en la figura *Filtros en la impresión en red* en la página 198.

Caso B3 Esta configuración es casi idéntica a la de un sistema autónomo con una impresora conectada localmente.

En la figura *Filtros en la impresión en red* en la página 198 se muestra la configuración de un sistema autónomo con fines comparativos:

Al observar retrospectivamente cada uno de los ejemplos de configuración empezando por el final, se ve la evolución de un sistema autónomo con una impresora local a una configuración más compleja para múltiples estaciones de

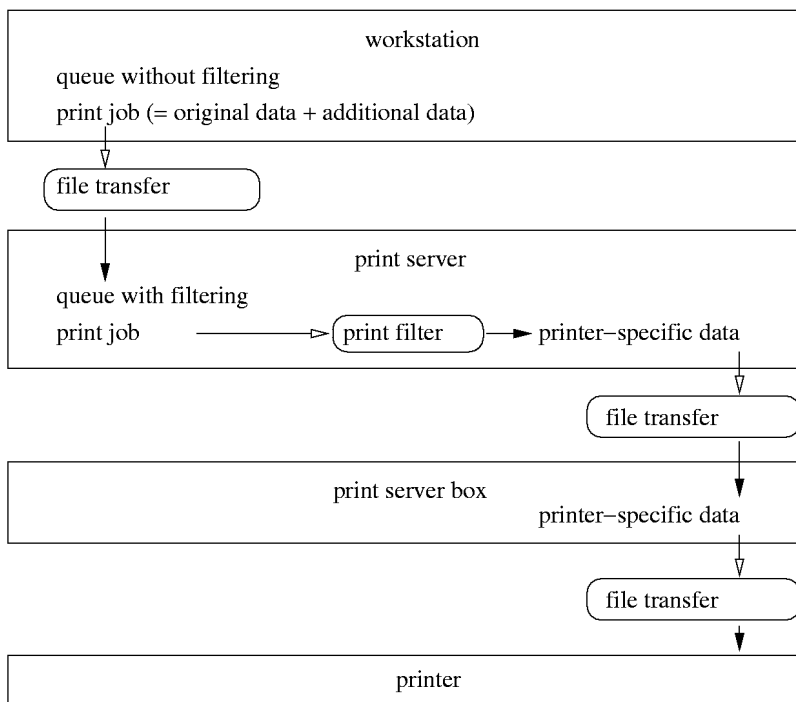


Figura 6.5: Configuración 2

trabajo con un servidor de impresión para varias impresoras de red/servidores de impresión dedicados.

Resolución de problemas

Comprobar la red TCP/IP La red TCP/IP, resolución de nombres incluida, debe funcionar adecuadamente.

Comprobar la configuración del filtro Conecte la impresora directamente al primer puerto paralelo del ordenador, configurándola como impresora local para evitar posibles problemas con la red (sólo durante la prueba). Una vez que la impresora funciona localmente, ya conoce el controlador de Ghostscript y los demás parámetros para la configuración del filtro.

Comprobar el lpd remoto El siguiente comando le permite comprobar si es

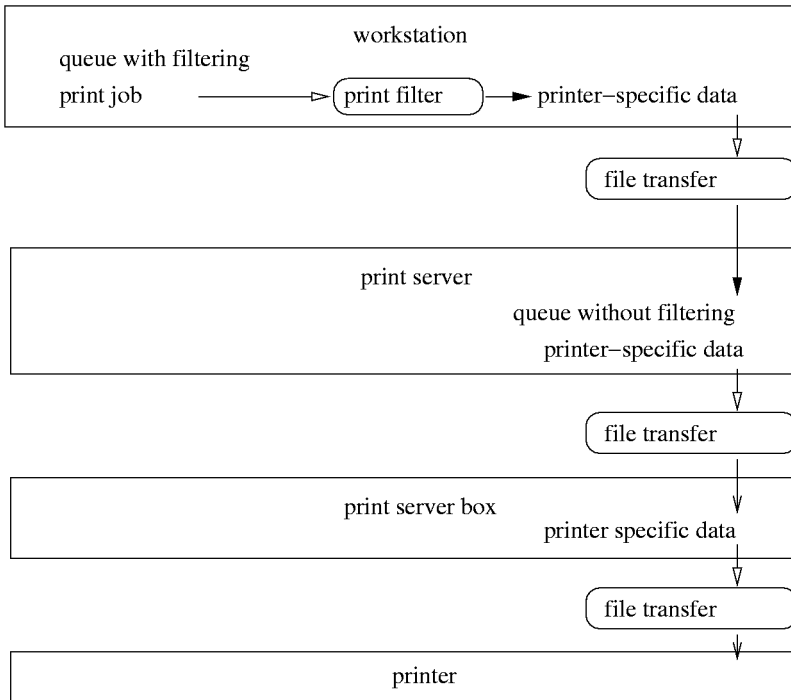


Figura 6.6: Configuración 3

posible una conexión TCP a lpd (puerto 515) en el ordenador *<host>*:

```
netcat -z <host> 515 && echo ok || echo failed
```

Si no lo es, o bien no funciona el lpd, o existen problemas importantes en la red.

Como usuario `root` se puede solicitar un informe (que puede llegar a ser muy largo) sobre el estado de la cola de impresión *<queue>* en un ordenador (remoto) *<host>*, siempre que el lpd remoto esté funcionando y sea accesible:

```
echo -e "\004<queue>" \
| netcat -w 2 -p 722 <host> 515
```

Si no se recibe respuesta del lpd puede que no funcione el lpd o que haya problemas importantes en la red. Si hay respuesta del lpd esta debería aclarar por qué no se puede imprimir a la cola de impresión *queue* del

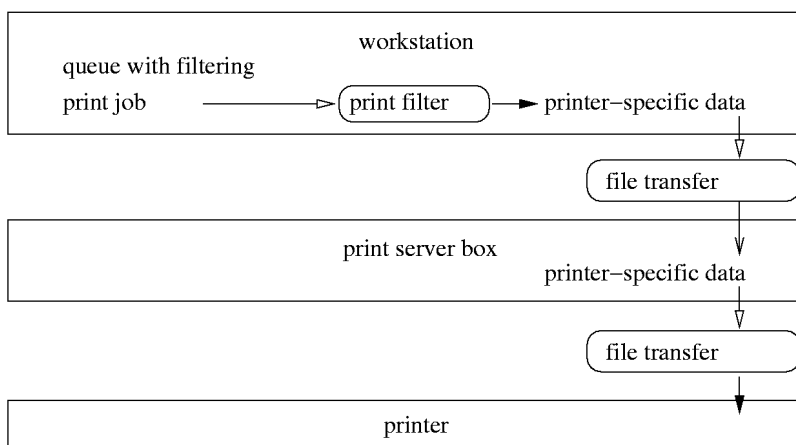


Figura 6.7: Configuración 4

ordenador host- Ejemplos:

```

lpd: your host does not have line printer access
lpd: queue does not exist
printer: spooling disabled
printer: printing disabled

```

Mensaje en pantalla 11: Mensaje de error de lpd

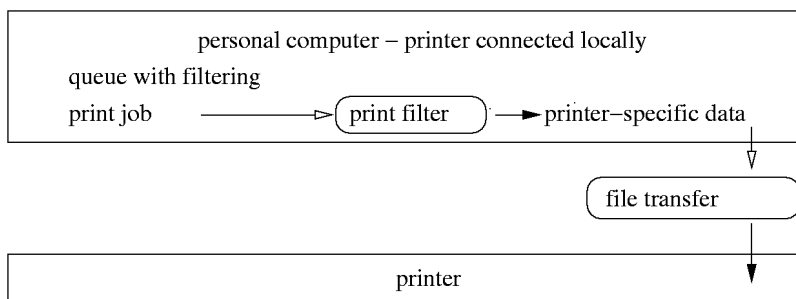


Figura 6.8: Configuración 5

Si se recibe tal respuesta del lpd, se trata de un problema del lpd remoto.

Comprobar un cupsd remoto Con el siguiente comando se puede comprobar si en la red existe un servidor de red CUPS, ya que éste debería anunciar su cola de impresión por broadcast a través del puerto UDP 631 cada 30 segundos.

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

Después de 40 segundos de espera se produce una salida semejante a ésta cuando el servidor de red CUPS realiza el broadcast:

```
... ipp://<host>.<domain>:631/printers/<queue>
```

Mensaje en pantalla 12: Broadcast del servidor de red CUPS

El siguiente comando permite comprobar si es posible establecer una conexión TCP al cupsd (puerto 631) del ordenador *<host>*:

```
netcat -z <host> 631 && echo ok || echo failed
```

Si no lo es, o no funciona el cupsd o existen problemas importantes en la red.

```
lpstat -h <host> -l -t
```

Con este comando se puede solicitar un informe (que a veces puede llegar a ser muy largo) del estado de todas las colas de impresión del ordenador *<host>*, siempre que haya un cupsd en funcionamiento y que sea posible conectarse con él.

```
echo -en "\r" \  
| lp -d <queue> -h <host>
```

Con este comando se puede comprobar si la cola de impresión *<queue>* del ordenador *<host>* acepta un trabajo de impresión compuesto por un único signo de retorno de carro. Es decir, es sólo una prueba y no debería imprimirse nada. En caso de imprimirse, el resultado será sólo una hoja en blanco.

Comprobar un servidor SMB remoto El funcionamiento básico puede comprobarse con el siguiente comando:

```
echo -en "\r" \  
| smbclient '//<HOST>/<SHARE>' ' <PASSWORD>' \  
-c 'print -' -N -U ' <USER>' \  
\
```

```
&& echo ok || echo failed
```

Introduzca en *<HOST>* el nombre del ordenador del servidor Samba, en *<SHARE>* el nombre de la cola de impresión remota (el nombre del directorio compartido Samba); en *<PASSWORD>* la contraseña y en *<USER>* el nombre de usuario. Aquí se trata sólo de una prueba y no debería imprimirse nada; pero en caso de imprimirse, el resultado será únicamente una hoja en blanco.

Con el siguiente comando se muestran los shares o directorios compartidos disponibles en el ordenador *<host>* — véase página del manual de *smbclient* (*man smbclient*):

```
smbclient -N -L <host>
```

La impresora de red o el servidor de impresión dedicado no funcionan correctamente.

A veces hay problemas con el spooler de impresión que se ejecuta en el servidor de impresión dedicado cuando se incrementa el volumen de impresión. Puesto que es un problema del spooler en el servidor de impresión dedicado o en la impresora de red, no se puede hacer nada. Sin embargo, existe la posibilidad de evitar el spooler del servidor de impresión dedicado comunicándose directamente a través del socket TCP con la impresora conectada al servidor de impresión dedicado.

De esta forma, el servidor de impresión dedicado sólo funciona como conversor entre las distintas formas de transmisión de datos (red TCP/IP y conexión local a la impresora). Así la impresora conectada al servidor de impresión dedicado se comporta como una impresora local. Asimismo el control sobre la impresora es más directo que el que se tendría si el spooler estuviera funcionando. Para esto debe conocerse el puerto TCP correspondiente del servidor de impresión dedicado. Con la impresora encendida y conectada al servidor de impresión dedicado, este puerto TCP se puede averiguar normalmente con el programa *nmap* del paquete *nmap* poco después de haber arrancado el servidor de impresión dedicado.

Este es el ejemplo de la salida de *nmap* con 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

La salida significa:

- Es posible registrarse en el servidor de impresión dedicado vía `telnet`. Allí puede solicitar información general y realizar configuraciones básicas.
- Vía HTTP es posible comunicarse con un servidor web que esté en funcionamiento en el servidor de impresión dedicado. Éste normalmente proporciona información detallada y permite realizar configuraciones avanzadas.
- Es posible comunicarse con el spooler de impresión que está en funcionamiento en el servidor de impresión dedicado a través del puerto 515 mediante el protocolo LPD.
- Es posible comunicarse con el spooler de impresión que está en funcionamiento en el servidor de impresión dedicado a través del puerto 631 y utilizando el protocolo IPP.
- Es posible comunicarse con la impresora conectada al servidor de impresión dedicado a través del puerto 9100 y utilizando un socket TCP.

Servidor de impresión LPD e IPP

LPD, IPP y CUPS

Aunque por lo general un servidor CUPS sólo soporta el protocolo IPP, el programa `/usr/lib/cups/daemon/cups-lpd` del paquete `cups` permite que un servidor CUPS pueda aceptar trabajos de impresión que le han sido enviados al puerto 515 mediante el protocolo LPD. Para ello se debe activar el servicio correspondiente para `xinetd` — normalmente con `YAST` o manualmente activando la línea correspondiente en el archivo `/etc/xinetd.d/cups-lpd`.

LPRng/lpfilter y CUPS

Puede ocurrir que desee ejecutar ambos sistemas de impresión LPRng/lpfilter y CUPS en el mismo ordenador, ya sea por ampliar un servidor de impresión LPD con CUPS, o porque en algunos casos sea necesario el sistema LPRng/lpfilter.

En principio se presentan dificultades cuando los dos sistemas de impresión se ejecutan en el mismo ordenador. Aquí se expondrá brevemente los problemas y limitaciones que pueden ocurrir. No obstante, este tema es demasiado complejo y no es posible ofrecer una solución en estas páginas.

- La configuración de la impresora no se debe realizar con YqST ya que la configuración de YqST no ha sido diseñada para estos casos.
- Existe un conflicto entre los paquetes `lprng` y `cups-client` debido a que contienen archivos con el mismo nombre p. ej. `/usr/bin/lpr` y `/usr/bin/lp`. Por eso el paquete `cups-client` no debe estar instalado. La consecuencia es que no hay herramientas CUPS de línea de comandos disponibles, sino sólo para LPRng. Sin embargo, es posible imprimir desde una interfaz gráfica con `xpp` o `kprinter` en colas de impresión CUPS, así como desde todas las aplicaciones que soportan CUPS directamente.
- Por lo general, al arrancar, `cupsd` vuelve a crear el archivo `/etc/printcap` que sólo contiene los nombres de todas las colas de impresión CUPS. Esto ocurre por razones de compatibilidad, ya que muchas aplicaciones leen las colas de impresión de `/etc/printcap` para poder ofrecerlas en el menú de impresión. Este servicio debe ser desactivado para `cupsd` de tal forma que `/etc/printcap` sólo esté disponible para LPRng/lpdfilter. La consecuencia es que las aplicaciones que sólo utilizan los nombres de colas de impresión que se encuentran en `/etc/printcap` sólo mostrarán las colas locales, pero no las colas CUPS disponibles en la red.

Hotplug

Con el transcurso del tiempo se han comenzado a usar componentes de hardware que se pueden conectar y desconectar mientras el ordenador está en funcionamiento. Junto con USB, un ejemplo conocido, se encuentran también PCI, PCMCIA, Firewire, SCSI y otras conexiones.

Los sistemas hotplug reconocen nuevo hardware añadido con el fin de configurarlo automáticamente y hacerlo disponible. Asimismo, se debe preparar a los componentes extraíbles para esta extracción o volver a dejar libres los recursos, en caso de que se retiren los componentes sin previo aviso.

Hotplug en Linux	204
Arrancar Hotplug y Coldplug	204
USB	205
PCI y PCMCIA	206
Red	207
Otros dispositivos y el desarrollo posterior	208

Hotplug en Linux

Es habitual que las partes de un sistema denominadas daemon controlen sucesos externos; por ello p. ej. `inetd` controla las solicitudes de la red. El daemon en `hotplug` es el mismo kernel. Para ello el controlador de un bus debe ser capaz de detectar nuevos dispositivos y comunicar su presencia al sistema de manera uniforme. En el kernel 2.4 esto lo puede hacer USB, PCMCIA, Firewire, PCI parcialmente y el subsistema de red. Esta parte de `hotplug` está integrada en los módulos correspondientes y no se puede tocar sin realizar cambios en el kernel.

Atención

Hotplug sólo maneja dispositivos PCMCIA si se trata de tarjetas CardBus y se elige el kernel del sistema PCMCIA, por lo que aparecerán como dispositivos PCI. Más información en la sección sobre PCMCIA.

Atención

La segunda parte de `hotplug` nos guía por los pasos necesarios para insertar o desconectar dispositivos, y consiste en una serie de scripts que se encuentran en el directorio `/etc/hotplug` junto con el script principal `/sbin/hotplug`. Este script es el punto de conexión entre el kernel y la serie de scripts de `hotplug`. A lo largo de este capítulo designaremos a estos scripts como "sistema `hotplug`".

Cuando se inserta o extrae un dispositivo `hotplug`, el kernel llama al script `/sbin/hotplug` y le da información adicional sobre los correspondientes componentes de hardware. Este script divide el trabajo, según el tipo de hardware, en más scripts, los cuales cargan o descargan el módulo del kernel y llaman a su vez a otros programas para la configuración de los componentes. Los programas están en `/etc/hotplug` y siempre acaban con `.agent`.

Arrancar Hotplug y Coldplug

A pesar de que el kernel siempre envía los sucesos de `hotplug` a `/sbin/hotplug`, el sistema `hotplug` primero debe ser arrancado con el comando `rchtplug start`. Mientras no se arranque `hotplug`, se desecharán todos los sucesos correspondientes.

Además hay componentes reconocidos por el kernel incluso antes de que sea posible el acceso al sistema de archivos. Estos acontecimientos se pierden sin más. Por tanto en los scripts `/etc/hotplug/*.rc` se intenta crear de forma artificial los acontecimientos correspondientes al hardware que ya está disponible. Aquí es donde también se habla de "Coldplug".

Si llegados a este punto aún no se ha cargado el módulo base USB, estos se cargarán y se colgará el sistema de dispositivos USB (usbdevfs).

Si se para hotplug con `rchotplug stop`, no se analizará ningún otro suceso. Si no piensa cambiar el hardware de su sistema mientras trabaje con él, puede desactivar hotplug con toda tranquilidad. Sin embargo se debe configurar dispositivos USB y PCMCIA de otra forma.

En el directorio `/etc/sysconfig/hotplug` hay algunas variables que controlan el comportamiento de hotplug. Así, p. ej. con la variable `<HOTPLUG_DEBUG>` se puede modificar la "comunicabilidad" de hotplug. Las variables `<HOTPLUG_START_USB>`, `<HOTPLUG_START_PCI>` y `<HOTPLUG_START_NET>` pueden fijarse para que sólo manejen acontecimientos de un tipo determinado. Todas las demás variables aparecen en la sección correspondiente.

Todos los mensajes de hotplug quedan registrados en el archivo (`/var/log/messages`) (log del sistema).

USB

Si ha insertado un dispositivo USB, el script `/etc/hotplug/usb.agent` proporciona un controlador adecuado y se asegura de que se cargue. Este controlador no tiene por qué ser un módulo del kernel, y así es como muchas cámaras USB se comunican directamente con la aplicación correspondiente.

La asignación de controladores al hardware sucede en varias etapas. En la primera etapa se comprueba en el archivo `/etc/hotplug/usb.usermap` si existe una aplicación o un script de inicio especial que se haga cargo del hardware. En caso de que no, se busca en `/etc/hotplug/usb.handmap` una posible asignación a un módulo del kernel. Si tampoco se encuentra nada allí, (lo que sucede en la mayor parte de los casos) se acude a la tabla de asignación del kernel `/lib/modules/<versiónkernel>/modules.usbmap`. Aquí se realiza un nuevo escaneo del hardware USB, que desencadena nuevas acciones al utilizarse KDS como interfaz gráfica. p. ej. a los dispositivos que se utilizan por primera vez, se les ofrece un módulo propio YaST para la configuración, o se arrancan determinadas aplicaciones para el uso de este dispositivo. Este mecanismo funciona paralelamente a otras acciones desencadenadas por `/etc/hotplug/usb.agent`.

usb.agent se encarga de manejar los dispositivos USB dependiendo del tipo:

Dispositivos de almacenamiento como p. ej. discos duros, manejados por el script `/usr/sbin/checkhotmounts`, una vez cargado el controlador adecuado.

Dispositivos de red desencadenan un acontecimiento hotplug en el kernel, tras haber sido dados de alta. `usb.agent` tan sólo deja información del hardware, que el tráfico de la red utilizará más tarde. Se trata de una solución pasajera para el kernel 2.4 que no funciona cuando se utilizan más de un dispositivo de red USB, lo cual no suele ocurrir.

Cámaras la comunicación con ellas se produce a través del mecanismo KDE/escaneo de hardware. Para ello aún se fijan los permisos de acceso a los archivos del dispositivo de un usuario dado de alta mediante `/etc/hotplug/usb/usbcam`, para que este pueda acceder con KDE.

Ratones sólo necesitan un módulo cargado para comenzar a utilizarlos inmediatamente.

Teclado ya son necesarios en el arranque por lo que hotplug no se encarga de ellos.

RDSI/Módem en la actualidad aún no se configura automáticamente.

Aún hay algunas variables específicas USB en `/etc/sysconfig/hotplug`. En `<HOTPLUG_USB_HOSTCONTROLLER_LIST>` se encuentran los controladores para la controladora USB en el orden en que se intenta cargarlos. Si se carga un controlador adecuadamente, se introducen en `<HOTPLUG_USB_MODULES_TO_UNLOAD>` los módulos que se deberán descargar al extraer los componentes. No se descargará toda la sucesión de módulos USB porque no es posible determinar con exactitud si algún otro dispositivo los necesitará. La variable `<HOTPLUG_USB_NET_MODULES>` contiene los nombres de los módulos disponibles en una interfaz de red. En cuanto se cargue uno de estos módulos, se elaborará una descripción del hardware que será utilizada más tarde por el tráfico de la red. Este procedimiento quedará registrado en el log del sistema.

PCI y PCMCIA

Se debe diferenciar entre tarjetas PCMCIA, ya que a excepción de las tarjetas CardBus, hotplug no se encarga de tarjetas PC; y de aquellas solamente cuando el sistema PCMCIA del kernel está activo. Este estado de cosas se explica con más detalle en la sección de software (xxPCMCIA-SOFTWARExx) del capítulo PCMCIA.

Las tarjetas CardBus son, desde el punto de vista técnico, dispositivos PCI. Por ello, de ambas se encarga el mismo script `hotplug /etc/hotplug/pci`.

agent. Allí, se facilitará y cargará un controlador para la tarjeta. Además se dará la información sobre el lugar en el que se ha insertado la nueva tarjeta (PCI-Bus/PCMCIA-Slots y el número de slot), para que el posterior tráfico de red hotplug lea esta información y escoja la configuración correcta.

La asignación de controladores tiene dos etapas. Primero se busca en el archivo `/etc/hotplug/pci.handmap` configuraciones individuales y, en caso de que no se encuentren, se sigue buscando en la tabla de controladores PCI del kernel `/lib/modules/⟨versiónkernel⟩/modules.pcimap`. Si quiere cambiar la asignación de controladores, deberá cambiar también `/etc/hotplug/pci.handmap`, ya que se sobrescribirá la otra tabla al actualizar el kernel.

Contrariamente a USB, no se realizará ninguna acción especial dependiendo de que la tarjeta sea PCI o CardBus. Con tarjetas de red el kernel crea un suceso en la red hotplug, que da lugar a la configuración de la interfaz. Con el resto de las tarjetas se debe ejecutar las acciones manualmente.

En cuanto se extraen las tarjetas, se descargan los módulos utilizados..

En caso de que la descarga de determinados módulos cause problemas, esto se puede evitar introduciendo el nombre del módulo en la variable `⟨HOTPLUG_PCI_MODULES_NOT_TO_UNLOAD⟩` que se encuentra en `/etc/sysconfig/hotplug`.

Red

Una vez que se anuncia en el kernel el inicio o la terminación de una nueva interfaz de red, este crea un suceso hotplug en la red, que será utilizado por `/etc/hotplug/net.agent`. Allí sólo se tiene en cuenta las interfaces Ethernet, Tokenring y WirelessLAN. Para todos los otros tipos de redes, como módem o RDSI, existen otros mecanismos. Tampoco se trata aquí de las interfaces de red fijadas por tarjetas PCMCIA manipuladas por el gestor de tarjetas y no por hotplug. Aparecerá el mensaje correspondiente en el log del sistema.

Primero se intentará averiguar el hardware que la interfaz pone a disposición. Puesto que el kernel 2.4 no puede ofrecer dicha información, se utilizará la información ya elaborada por anteriores sucesos hotplug con USB o PCI. Aunque en la mayoría de los casos esto funciona correctamente, se debe considerar como una solución pasajera. Por tanto de hecho no está permitido insertar dos tarjetas de red simultáneamente. Si utiliza más de una tarjeta de red hotplug, conéctelas al ordenador una detrás de otra.

Basta con un intervalo entre una y otra de unos pocos segundos. Esta información queda registrada en `/var/log/messages`.

Con esta información sobre el hardware se llama el script `/sbin/ifup` (o `ifdown`). `ifup` puede asignar la configuración correcta a una determinada tar-

jeta, incluso cuando la interfaz tiene otro nombre. De hecho el kernel no asigna los nombres de interfaces siguiendo unas reglas.

También se pueden anotar en `/sbin/ifup` otras acciones individuales que se pueden ejecutar después de haber establecido una nueva interfaz de red. Más detalles en las páginas `man` sobre página del manual de `ifup` (`man ifup`). También es posible utilizar diferentes rutas por defecto según el hardware conectado; véase página del manual de `route` (`man route`).

En caso de que falle la indagación del hardware que se encuentra tras la interfaz (p. ej. con un Firewire) y que sólo se utilice un dispositivo de red hotplug, se puede introducir la descripción del hardware de red en la variable `<HOTPLUG_NET_DEFAULT_HARDWARE>` que se encuentra en `/etc/sysconfig/hotplug`. Se debe utilizar esta cadena de signos se debe corresponder con `/sbin/ifup` para la asignación de la configuración adecuada. En la variable `<HOTPLUG_NET_TIMEOUT>` se puede fijar cuánto tiempo debe esperar `net.agent` a que se produzca una descripción dinámica del hardware.

Otros dispositivos y el desarrollo posterior

No se soportan los tipos de hardware hotplug que no se hayan descrito aquí. Sin embargo hotplug se está desarrollando enormemente en la actualidad, lo cual depende en gran medida de las utilidades del kernel. Se espera que con la nueva versión del kernel 2.6 se puedan ofrecer nuevas utilidades.

Ordenadores portátiles

– PCMCIA, APM, IrDA

Los ordenadores portátiles suelen incorporar dispositivos especiales como p. ej. interfaces de infrarrojo (IrDA), tarjetas PCMCIA o la administración avanzada de potencia "Advanced Power Management" (APM). Estos componentes se encuentran a veces también en los ordenadores de sobremesa y no se distinguen mucho de los específicos que incorporan los portátiles. Por eso su configuración y su uso se encuentran resumidos en este capítulo.

PCMCIA	210
SCPM – System Configuration Profile Management	222
APM y ACPI – Powermanagement	230
IrDA – Infrared Data Association	244

PCMCIA

PCMCIA es la abreviatura de "Personal Computer Memory Card International Association" y se usa generalmente para todo el hardware y software relacionado con ello.

El hardware

El componente clave es la tarjeta PCMCIA, de la que se distinguen dos tipos diferentes:

Tarjetas PC Son las tarjetas que se emplean más a menudo y usan un bus de 16 bits para la transferencia de datos. Estas tarjetas suelen ser económicas y por lo general son estables y no presentan problemas.

Tarjetas CardBus Son tarjetas de un estándar más nuevo con un bus de 32 bits de anchura, por lo que son más rápidas pero también más caras. El gasto adicional de estas tarjetas normalmente no está justificado, ya que el cuello de botella de la transferencia de datos suele estar en otra parte, y no en el bus. Ya existen varios drivers para estas tarjetas; aunque algunos de ellos aún son inestables (en función de la combinación de la controladora PCMCIA y la tarjeta).

Cuando el servicio PCMCIA está activo, el comando `cardctl identify` indica la tarjeta introducida en la ranura. Una lista de las tarjetas soportadas se encuentra en `SUPPORTED.CARDS` en el fichero `/usr/share/doc/packages/pcmcia`. Allí se encuentra también la última versión del `PCMCIA-HOWTO`.

El segundo componente que se necesita para el soporte PCMCIA es la controladora o bien el PC-Card/CardBus-Bridge. Este puente establece la comunicación entre la tarjeta y el bus PCI o (en caso de máquinas antiguas) el bus ISA. Casi siempre las controladoras son compatibles con el chip i82365 de Intel por lo que todos los modelos corrientes se soportan. Con el comando `probe` se puede averiguar el tipo de controladora. Si la controladora conecta al bus PCI se puede conseguir más información con `lspci -vt`.

El software

Diferencias entre los dos sistemas PCMCIA

Existen dos sistemas PCMCIA: el externo y el integrado en el kernel. El sistema PCMCIA externo de David Hinds es el más antiguo, por lo que ha sido probado

y mejorado durante más tiempo. Las fuentes de los módulos que emplea no están integrados en las del kernel, y es por esto por lo que se denomina sistema "externo". Sin embargo, a partir del kernel 2.4, existe otro módulo alternativo en las fuentes: las del sistema PCMCIA integrado en el kernel. Los módulos básicos fueron escritos por Linus Torvalds y soportan mejor los puentes Cardbus más nuevos.

Desgraciadamente, ambos sistemas son incompatibles. Además, en ambos sistemas se encuentran entradas diferentes para los drivers. Por esta razón, dependiendo del hardware, sólo se puede emplear uno de los dos sistemas. La norma en SuSE Linux es utilizar el PCMCIA integrado en el kernel, aunque también se puede cambiar de sistema. Para ello, se debe asignar a la variable `(PCMCIA_SYSTEM)` el valor `external` o `kernel`, y después arrancar de nuevo PCMCIA con `rcpcmcia restart`. Para un cambio temporal también se puede utilizar `rcpcmcia [re]start external, kernel`. Puede encontrar información más detallada en `/usr/share/doc/packages/pcmcia/README.SuSE`.

El módulo base

El módulo del kernel de ambos sistemas se encuentra en el paquete del kernel. También se necesitan el paquete `pcmcia` y `hotplug`.

Al arrancar un PCMCIA se cargan los módulos `pcmcia_core`, `i82365` (PCMCIA externo) o `yenta_socket` (PCMCIA integrado en el kernel) y `ds`.

En muy raras ocasiones se necesita el módulo `tcic` en vez de `i82365` o `yenta_socket`. Estos inicializan las controladoras PCMCIA que se encuentran disponibles y proporcionan funciones básicas.

El administrador de tarjetas

Para que las tarjetas PCMCIA puedan intercambiarse, debe existir un Daemon que controle la actividad de las ranuras de conexión. Según el sistema PCMCIA elegido y el hardware utilizado, esta tarea será realizada por el administrador de tarjetas (ingl. *cardmanager*) o por el sistema Hotplug del kernel. Para los PCMCIA externos se emplea el administrador de tarjetas. En el caso de los PCMCIA integrados en el kernel, el administrador sólo manipula la tarjeta PC, mientras que las tarjetas CardBus son controladas por Hotplug. El script de arranque del PCMCIA inicia el administrador de tarjetas después de que el módulo básico se haya cargado. Puesto que el Hotplug también soporta otros subsistemas además del PCMCIA, dispone de un script de arranque propio. (Ver también el capítulo [Hotplug](#) en la página 203).

Cuando se introduce una tarjeta, el administrador de tarjetas o el Hotplug averigua el tipo y la función para cargar los módulos correspondientes. Una

vez que todos los módulos se hayan cargado correctamente y según la función de la tarjeta, el administrador de tarjetas o el Hotplug inicia determinados scripts de arranque que se encargan de establecer la conexión de red, de montar particiones de discos SCSI externos o llevan a cabo otras acciones específicas del hardware. Los scripts del administrador de tarjetas se encuentran en `/etc/pcmcia` y los del Hotplug en `/etc/hotplug`. Al retirar la tarjeta, tanto el administrador de tarjetas como el Hotplug se encarga de desactivar, utilizando los mismos scripts, las diversas actividades de la tarjeta. Finalmente, los módulos que ya no se necesitan se descargan de la memoria.

Tanto los protocolos de inicio de los sistemas PCMCIA como todas las acciones de la tarjeta quedan guardados en el archivo log del sistema (`/var/log/messages`). Allí se puede comprobar el sistema PCMCIA, el daemon y el script utilizados para la instalación. En teoría una tarjeta PCMCIA puede retirarse fácilmente, especialmente si se trata de una tarjeta RDSI, de módem o de red, siempre que ya se hayan acabado las conexiones a la red. Sin embargo no funciona en combinación con particiones de un disco externo o con directorios NFS. En este caso se debe tener un cuidado especial para que las unidades estén sincronizadas y se desmonten correctamente. Por supuesto, esto no es posible cuando la tarjeta ya se ha sacado. En caso de duda, utilice

```
cardctl eject
```

Esta orden desactiva todas las tarjetas que se encuentren en el portátil. Si quiere desactivar solamente una tarjeta, añada el número de slot.
p.ej. `cardctl eject 0`.

La configuración

Para especificar si se debe iniciar el PCMCIA o Hotplug al encender el ordenador, utilice el editor de runlevels de YaST2 o escriba `chkconfig` en la línea de comandos.

En el `/etc/sysconfig/pcmcia` se encuentran cuatro variables:

⟨`PCMCIA_SYSTEM`⟩ determina el sistema PCMCIA que se empleará.

⟨`PCMCIA_PCIC`⟩ incluye el nombre del módulo hacia el que se dirige la controladora PCMCIA. En casos normales, el script de inicio ya facilita este nombre, y esta variable queda vacía. Introduzca aquí el módulo sólo si se producen errores.

⟨`PCMCIA_CORE_OPTS`⟩ está pensada como parámetro para el módulo `pcmcia_core`, pero casi nunca es necesario utilizarlo. Estas

opciones están descritas en página del manual de `pcmcia_core` (`man pcmcia_core`).

(`PCMCIA_PCIC_OPTS`) recoge el parámetro para el módulo `i82365`.

También para este caso existe una página del manual de `i82365` (`man i82365`). Si se utiliza `yenta_socket`, olvídense de estas opciones, puesto que `yenta_socket` no reconoce ninguna opción.

La disposición de los drivers de las tarjetas PCMCIA para el administrador de tarjetas se encuentra en los ficheros `/etc/pcmcia/config` y `/etc/pcmcia/*.conf`. En primer lugar se lee `config` y después `/*.conf` siguiendo un orden alfabético. La última entrada para una tarjeta es la decisiva. Los detalles sobre la sintaxis se encuentran en la página del manual de `pcmcia` (`man pcmcia`).

La disposición de los drivers de las tarjetas PCMCIA para Hotplug se describen en el capítulo que trata sobre Hotplug (ver [Hotplug](#) en la página 203).

Tarjetas de red (Ethernet, Wireless LAN y TokenRing)

Estas tarjetas se pueden instalar como tarjetas de red corrientes con YaST2, escogiendo la opción 'PCMCIA' en tipo de tarjeta. Todos los detalles adicionales de la configuración de red se encuentran en el capítulo sobre la conexión a red. Preste atención a las indicaciones para las tarjetas que funcionan con Hotplug.

RDSI

La configuración de las tarjetas PC RDSI funciona en gran medida como la del resto de tarjetas RDSI con YaST. No importa cuál de las dos tarjetas RDSI PCMCIA se escoja; lo que importa es que sea una tarjeta PCMCIA. Al configurar el hardware y el proveedor, compruebe que el modo de funcionamiento es `hotplug` y no `onboot`.

También existen módems RDSI para tarjetas PCMCIA. Son tarjetas de módem o multitarea que incorporan un kit de conexión RDSI y se comportan como un módem.

Módem

Las tarjetas PC de módem normalmente no conocen ninguna configuración específica para PCMCIA. Cuando se inserta un módem, este está directamente disponible en `/dev/modem`.

También existen los llamados Softmodems para las tarjetas PCMCIA, pero por lo general no los soportan. En caso de que exista un driver, debe unirse al sistema de forma individual

SCSI e IDE

El administrador de tarjetas o Hotplug carga el módulo adecuado. Nada más insertar una tarjeta SCSI o IDE, se encuentran disponibles los dispositivos asociados, cuyos nombres se averiguan dinámicamente. Puede encontrar más información sobre los dispositivos SCSI e IDE disponibles en `/proc/scsi` o `/proc/ide`.

Los discos duros externos, los lectores CD-ROM y otros dispositivos similares deben estar encendidos antes de introducir la tarjeta PCMCIA. La terminación de los dispositivos SCSI debe realizarse de forma activa.

Atención

Hay que desmontar todas las particiones de los dispositivos que estén conectados a una tarjeta SCSI o IDE antes de extraerla. En caso de haberlo olvidado, no se puede acceder a estos dispositivos antes de un reinicio del sistema, aunque el resto del sistema funcione perfectamente.

Atención

Puede instalar Linux completamente en un disco duro externo, pero el procedimiento de arranque resulta un poco más complicado. En todo caso se necesita un disquete de arranque que incluya el kernel y un Ramdisk inicial `initrd`; más información en el apartado *Arrancar con initial ramdisk* en la página 273. La `initrd` contiene un sistema de ficheros virtual con todos los módulos y programas necesarios para el soporte PCMCIA. El disquete de arranque y las imágenes de este disquete tienen esta misma estructura, lo que le permite arrancar siempre la instalación externa mediante estos disquetes. La desventaja es que se debe cargar manualmente el soporte PCMCIA en cada inicio. Para los usuarios avanzados existe la posibilidad de generar un disquete de arranque hecho a medida. Puede encontrar más información en inglés en el PCMCIA-HOWTO del apartado 5.3 *Booting from a PCMCIA device*.

Configuración variable - SCPM

A menudo un ordenador portátil necesita configuraciones diferentes dependiendo del lugar en el cual debe operar (p. ej. en el trabajo o en casa).

Gracias a los esquemas PCMCIA, se puede realizar fácilmente con dispositivos PCMCIA. Puesto que los drivers de las tarjetas de red incluidas o de los dispositivos USB-FireWire también requieren perfiles distintos para la configuración del sistema, existe desde Linux 8.0 el paquete SCPM (System Configuration Profile Management). Esta es la razón de que SuSE no dé soporte a los esquemas PCMCIA. No obstante, si Vd. quiere seguir empleando estos esquemas, debe realizar manualmente la configuración en `/etc/pcmcia`. De todas formas, le aconsejamos que cambie a SCPM, para que pueda administrar la parte de la

configuración del sistema que desee, y no sólo las que estén relacionadas con PCMCIA.

La documentación sobre SCPM se encuentra en el apartado *SCPM – System Configuration Profile Management* en la página 222.

Si aún no funciona

Puede ocurrir que haya problemas con el uso de PCMCIA en algunos ordenadores portátiles o en combinación con determinadas tarjetas. La mayoría de las problemas se pueden solucionar sin demasiado esfuerzo, siempre que se proceda sistemáticamente.

Aviso

Puesto que en SuSE Linux coexisten tanto PCMCIA externos como integrados en el kernel, se debe tener en cuenta una peculiaridad al cargar los módulos manualmente. Ambos sistemas PCMCIA emplean módulos que tienen el mismo nombre pero que se encuentran en subdirectorios diferentes en `/lib/modules/<kernelversion>`. Estos subdirectorios se llaman `pcmcia` para el PCMCIA integrado en el kernel y `pcmcia-external` para el PCMCIA externo. Por lo tanto, al cargar estos módulos manualmente se debe indicar el subdirectorio correspondiente, ya sea `insmod /lib/modules/<versión del kernel>/<subdirectorio>/<nombre de archivo del módulo>` o `modprobe -t <subdirectorio> <nombre del módulo>`.

Aviso

Lo primero es averiguar si la causa del problema está relacionada con una tarjeta o con el sistema base PCMCIA. Por eso hay que iniciar el ordenador sin ninguna tarjeta insertada. Todos los mensajes de interés se protocolizan en el fichero `/var/log/messages`; por lo que es necesario observar este fichero mientras se realicen las pruebas con:

```
tierra:~ # tail -f /var/log/messages
```

lo que permite determinar uno de los siguientes casos como causa del error.

El sistema base PCMCIA no funciona

Si el sistema llega a pararse durante el arranque con el mensaje PCMCIA: "Starting services" o si hay otras incidencias extrañas, se puede deshabilitar el servicio PCMCIA para el próximo arranque, indicando `NOPCMCIA=yes` en la ventana de arranque.

Para conocer mejor la causa del error, se deben cargar manual y secuencialmente los tres módulos básicos. Para ello, se usan los comandos

```
tierra:~ # modprobe -t <dir> pcmcia_core
tierra:~ # modprobe -t pcmcia-external i82365 (para PCMCIA externos)
tierra:~ # modprobe -t pcmcia yenta_socket (para PCMCIA en kernel)
```

o – en pocas ocasiones –

```
tierra:~ # modprobe -t <dir> tcic
```

y

```
tierra:~ # modprobe -t <dir> ds
```

Los módulos críticos son los dos primeros.

La página man `pcmcia_core` presta ayuda cuando el error aparece en el momento de cargar `pcmcia_core`. Las opciones que se mencionan en la página del manual se pueden usar en combinación con el comando `modprobe`. Como ejemplo, se puede deshabilitar el soporte APM de los módulos PCMCIA, ya que en pocos casos resulta problemático. Para realizarlo existe la opción `doapm`; con `do_apm=0` se desactiva la gestión de potencia:

```
modprobe -t <dir> pcmciacore do_apm=0
```

Una vez que la opción probada tenga éxito, esta se guarda en el fichero `/etc/sysconfig/pcmcia` mediante la variable `<PCMCIA_CORE_OPTS>`:

```
PCMCIA_CORE_OPTS="do_apm=0"
```

En muy pocas ocasiones, la comprobación de áreas de memoria libres es problemática, debido a interferencias con los componentes del hardware. Para evitar esto, se puede utilizar `probe_io=0`. Para combinar varias opciones, éstas se han de separar con un espacio en blanco:

```
PCMCIA_CORE_OPTS="do_apm=0 probe_io=0"
```

Para resolver problemas que surjan al cargar los módulos `i82365`, se puede recurrir a la página del manual de `i82365` (man `i82365`).

Un problema típico a la hora de cargar este módulo es un conflicto de recursos, una interrupción, un puerto de E/S (I/O-Port) o un rango de memoria que se ocupa dos veces. En realidad el módulo `i82365` comprueba los recursos antes de asignarlos a la tarjeta pero justamente esta comprobación es la que a veces produce un error. Por ello, hay ordenadores que bloquean el teclado y/o el ratón en el momento de comprobar la interrupción 12 (dispositivos PS/2). En

tal caso sirve como remedio el parámetro `irq_list=<Liste von IRQs>`. La lista debe contener todos los IRQs que se pueden usar, Así:

```
modprobe i82365 irq_list=5,7,9,10
```

o, para fijarlo, en `/etc/sysconfig/pcmcia`:

```
PCMCIA_PCIC_OPTS="irq_list=5,7,9,10"
```

Además el administrador de tareas (ingl. *Cardmanager*) evalúa los ficheros `/etc/pcmcia/config` y `/etc/pcmcia/config.opts`. Los parámetros definidos en estos ficheros no tienen relevancia antes de la carga de los drivers para las tarjetas PCMCIA. En `/etc/pcmcia/config.opts` también se puede indicar las IRQs, los puertos E/S y los rangos de memoria a incluir o excluir. A diferencia de la opción `irqlist`, los recursos excluidos en `config.opts` no se usan para una tarjeta PCMCIA pero sí que se comprueban mediante el módulo base `i82365`.

La tarjeta PCMCIA no funciona (bien)

Fundamentalmente, hay tres razones por las que una tarjeta PCMCIA no funciona bien: no se reconoce la tarjeta, no se puede cargar el driver, o la interfaz que el driver pone a disposición está mal configurada.

Se debe comprobar que la tarjeta es manipulada por el administrador de tarjetas o por el Hotplug. Como recordatorio: el administrador gestiona los PCMCIA externos, el administrador de tarjetas PC-Card maneja los PCMCIA integrados en el kernel y Hotplug se encarga de las tarjetas Cardbus. Aquí sólo se trata del administrador de tarjetas. Los problemas con Hotplug se encuentran en el capítulo sobre Hotplug (ver capítulo [Hotplug](#) en la página 203).

■ No se reconoce la tarjeta.

Si no se reconoce la tarjeta, aparece el mensaje "unsupported Card in Slot x" en `/var/log/messages`. El mensaje sólo indica que el administrador de tarjetas no es capaz de asignar un driver a la tarjeta, ya que se necesita `/etc/pcmcia/config` o `/etc/pcmcia/*.conf` para esta asignación. Estos archivos son, por así decirlo, una base de datos de drivers, que se puede ampliar fácilmente usando entradas existentes como plantilla para las nuevas. Para identificar la tarjeta, puede emplear el comando `cardctl ident`. Para más información sobre el tema, consulte el apartado 6 del PCMCIA-HOWTO y la página del manual de `pcmcia` (`man pcmcia`). Después de modificar `/etc/pcmcia/config` o `/etc/pcmcia/*.conf` debe cargar de nuevo la disposición del driver mediante `rcpcmcia reload`.

■ El driver no se carga

Una de las causas es que exista una disposición incorrecta en la base de datos de drivers. Esto puede ocurrir p. ej. si el fabricante ha insertado un chip distinto en un modelo de tarjeta que no ha cambiado externamente. A veces se dispone de drivers opcionales, que funcionan mejor (o exclusivamente) con modelos distintos al driver especificado. En estos casos, se necesita información exacta sobre la tarjeta. También sirve de ayuda preguntar en listas de correo o en el Servicio de Soporte Avanzado (ingl. *Advanced Support Service*).

Otra causa puede ser un conflicto de recursos. Con la mayoría de las tarjetas PCMCIA no importa qué IRQ, puerto E/S o rango de memoria utilizan, pero hay excepciones. Por eso, se debe siempre probar una tarjeta y, en determinadas ocasiones también, desconectar temporalmente otros componentes del sistema p. ej. tarjetas de sonido, IrDA, módems e impresoras. Se puede ver la distribución de recursos del sistema con `lsdev`. (Es normal que varios dispositivos PCI empleen el mismo IRQ).

Una posible solución consiste en emplear la opción adecuada para el módulo `i82365` (ver arriba en `PCMCIA_PCIC_OPTS`). No obstante, existen opciones para determinados drivers de tarjeta; dichas opciones se pueden averiguar en `/lib/modules/<directorio correcto pcmcia>/<driver>` (se necesita toda la ruta para dirigirse al sistema PCMCIA correspondiente). Para la mayoría de los módulos existe una página man. Consejo: `rpm -ql pcmcia | grep man` elabora una lista de todas las páginas del manual relacionadas con pcmcia. Para probar las opciones, los drivers de tarjeta se pueden cargar manualmente. Una vez más, compruebe que el módulo utiliza el sistema PCMCIA empleado. Lea el aviso que se encuentra más arriba.

Cuando encuentre la solución, se puede permitir o prohibir el empleo de un determinado recurso en `/etc/pcmcia/config.opts`; también se encuentran aquí las opciones para los drives de tarjeta.

Si p. ej. el módulo `pcnet_cs` sólo se puede gestionar con el IRQ 5, se deberá realizar la siguiente entrada:

```
module pcnet_cs opts irq_list=5
```

Un problema específico de las tarjetas de red 10/100 Mbit es una selección automática equivocada del modo de transferencia. El problema se puede remediar con el comando `ifport` o `mii_tool`, que permiten averiguar y modificar el modo de transferencia. Para que estos comandos se ejecuten automáticamente, es necesario adaptar individualmente el script `/etc/pcmcia/network`.

■ Interfaz mal configurada

En este caso, es aconsejable comprobar adecuadamente la configuración de la interfaz para descartar errores de configuración. Además, con tarjetas de red, se puede aumentar el rango de diálogo del script de red, mediante la asignación de la variable `DEBUG=yes` en `/etc/sysconfig/network/config`. Con otro tipo de tarjetas, o en caso de que sirva de ayuda, existe la posibilidad de incluir una línea `set -x` en el script que llama el administrador de tarjetas (ver `/var/log/messages`). De esta forma, cada comando del script quedará protocolizado en el log del sistema. Si encuentra la posición crucial en un script, puede introducir y probar dichos comandos en una terminal.

Instalación vía PCMCIA

En ciertas ocasiones ya se requiere el soporte PCMCIA en la instalación, al instalar a través de la red o al usar el CDROM mediante PCMCIA. Para ello se debe emplear un disquete de arranque, con lo que se empleará uno de los disquetes de módulo.

Después de arrancar con el disquete (o de haber elegido ‘Instalación manual’ al arrancar con CD) se inicia el programa `linuxrc`. Entonces, en el menú ‘Módulos del kernel (driver de hardware)’, se debe elegir la opción ‘Cargar driver PCMCIA’. En primer lugar, aparecen dos cuadros de diálogo que permiten introducir opciones para los módulos `pcmcia_core` y `i82365`. Normalmente estos campos se quedan vacíos. Las páginas man para `pcmcia_core` y `i82365` se encuentran en el primer CD como ficheros de texto dentro del directorio `docu`.

En SuSE Linux 8.2 está instalado, como en las versiones anteriores, el sistema PCMCIA externo.

Durante la instalación aparecen mensajes del sistema en las distintas consolas virtuales, a las que se puede acceder mediante (Alt)

+ (Teclas de función). Más adelante, cuando una interfaz gráfica esté activa, debe utilizar (Control) + (Alt) + (Teclas de función) .

También durante la instalación existen terminales en las que se puede ejecutar comandos. Mientras `linuxrc` está en funcionamiento, esta terminal se encuentra en la consola 9 (una shell muy rudimentaria); una vez cargado el sistema de instalación (YaST2 se ha iniciado), hay una `bash` y herramientas de sistema en la consola 2.

Si durante la instalación se ha cargado el driver equivocado para una tarjeta PCMCIA, se debe ajustar el disquete de arranque manualmente. Para ello, necesita tener conocimientos avanzados de Linux.

Después del primer paso de instalación, el sistema se reinicia total o parcialmente. Raras veces el sistema se para al iniciar PCMCIA, pero en este punto la instalación ya está tan avanzada que se puede iniciar Linux sin PCMCIA y en modo texto usando la opción de arranque `NOPCMCIA=yes`. Para solventar este problema consulte el apartado *Si aún no funciona* en la página 215.

Ocasionalmente, también se pueden realizar diversos ajustes del sistema en la consola 2, antes de que finalice la primera parte de la instalación, para que no sucedan fallos en el arranque.

Utilidades adicionales

El programa `cardctl` ya ha sido mencionado varias veces. Es la herramienta principal para conseguir información sobre PCMCIA, así como para ejecutar determinadas acciones. Puede encontrar detalles sobre el programa en `cardctl`. También se puede introducir `cardctl` para que aparezca una lista con los comandos válidos.

Para este programa también existe una interfaz gráfica `cardinfo` (ver figura 8.1), que permite controlar los aspectos más importantes. Sin embargo, el paquete `pcmcia-cardinfo` debe estar instalado.



Figura 8.1: El Programa Cardinfo

Otras utilidades del paquete `pcmcia` son `ifport`, `ifuser`, `probe` y `rcpcmcia`, pero no se usan con frecuencia. Para conocer exactamente el contenido completo del paquete `pcmcia`, se puede usar el comando `rpm -ql pcmcia`.

Actualizar el paquete Kernel o PCMCIA

Si quiere actualizar el kernel, utilice el paquete kernel ya preparado por SuSE. Si necesita compilar un kernel propio, también debe compilar el módulo PCMCIA.

Es esencial que el kernel nuevo ya se esté ejecutando, ya que cierta información se extrae de aquí. El paquete `pcmcia` ya debe estar instalado pero no iniciado; en

caso de duda, ejecute un `rpmcmcia stop`. Después instale el paquete fuente PCMCIA y a continuación introduzca:

```
rpm -ba /usr/src/packages/SPECS/pcmcia.spec
```

Ya está todo listo. En `/usr/src/packages/RPMS` se encuentra ahora un nuevo paquete. El paquete `pcmcia-modules` incluye los módulos PCMCIA para PCMCIA externos. Este paquete se debe instalar con `rpm -force`, ya que los archivos del módulo pertenecen oficialmente al paquete `kernel`.

Información adicional

Si está interesado en conocer más sobre el funcionamiento de determinados ordenadores portátiles, visite la Linux Laptop Homepage <http://linux-laptop.net>. Otra buena fuente de información es la TuxMobil Homepage <http://tuxmobil.org/> (TuxMobil – Ordenadores Móviles y Unix). Allí puede encontrar, además de información interesante, un Howto para ordenadores portátiles y otro para IrDA. También hay un artículo sobre ordenadores portátiles (PCMCIA) con Linux en la base de datos de soporte <http://sdb.suse.de/es/sdb/html/laptop.html> (o local en `file:/usr/share/doc/sdb/es/html/laptop.html`).

SCPM – System Configuration Profile Management

Hay situaciones en las que es necesario modificar la configuración del sistema. Esto ocurre a menudo en ordenadores portátiles con los que se trabaja desde lugares distintos. Pero también puede ocurrir que un ordenador de sobremesa utilice algunos componentes del hardware de forma temporal. O simplemente se quiere probar algo. En cualquier caso debería ser fácil volver al sistema de partida. Aún mejor si fuera posible volver a reproducir fácilmente la configuración modificada.

Hasta ahora esto sólo era posible con hardware PCMCIA. Allí se podían establecer distintas configuraciones en ciertos esquemas. Partiendo de esto hemos desarrollado SCPM, que anula la restricción a PCMCIA. Con “System Configuration Profile Management”, se puede configurar una parte de la configuración del sistema partiendo de diferentes perfiles de configuración. Dicho de otro modo, sería como sacar instantáneas de las distintas configuraciones del sistema, para que puedan volver a recrearse en cualquier momento. Y se puede escoger lo que se fotografía.

En los portátiles las aplicaciones principales dependen de la configuración de red. Pero con distintas configuraciones de red se puede cambiar en muchos casos otros elementos, p. ej. la configuración para correo electrónico o proxies. A esto se le añade la configuración de distintas impresoras en casa o en el trabajo, o la configuración especial XFree86, los distintos modos de ahorro de energía para cuando se está de viaje o en otra zona horaria.

Estas herramientas están cada vez más extendidas y deben cumplir más exigencias. Si tiene alguna crítica o sugerencia respecto a SCPM, no dude en ponerse en contacto con nosotros. Estamos muy interesados en su opinión. Hemos procurado fijar unos fundamentos flexibles para SCPM, para que también sea posible p. ej. el control de distintos perfiles de servidores. Contacte con nosotros en: <http://www.suse.com/feedback>

Fundamentos y conceptos básicos

A continuación se exponen unos conceptos básicos que se utilizarán en el resto de la documentación sobre SCPM y en el módulo YaST2.

- Por *Configuración del sistema* entendemos toda la configuración del ordenador; todas las configuraciones básicas, como p. ej. el uso de las particiones de los discos duros o configuraciones de red, selección de zona horaria o disposición del teclado.

- Un *Perfil* o *Perfil de configuración* es el estado de la configuración del sistema que ha quedado fijado y puede recrearse si se solicita.
- *Perfil activo* se refiere al último perfil activado. Eso no quiere decir que la configuración actual del sistema se corresponda exactamente con este perfil, puesto que la configuración puede modificarse en cualquier momento.
- *Recursos* en relación a SCPM son todos los elementos que contribuyen a la configuración del sistema. Puede tratarse de un archivo o de un enlace suave junto con los metadatos correspondientes, tales como usuarios, permisos, o tiempo de acceso. Pero también puede ser un servicio del sistema, que se ha ejecutado una vez y ha sido desactivado en otro perfil.
- Los recursos están organizados en *resource groups* o grupos de recursos. Estos grupos engloban recursos que concuerdan desde un punto de vista lógico. Esto se traduce para la mayoría de los grupos en que contienen un servicio y los archivos de configuración correspondientes. Este mecanismo permite agrupar los recursos manejados por SCPM sin que sea necesario saber qué archivos de configuración son requeridos para qué recursos. SCPM incluye ya una preselección de grupos de recursos activados que debería bastar para la mayoría de usuarios.

El gestor de perfiles de YaST y documentación adicional

Existe un módulo gráfico de YaST para SCPM que sirve de alternativa a la línea de comandos. Puesto que la funcionalidad de ambos es esencialmente la misma y es interesante para algunos fines conocer la pantalla de línea de comandos, aquí sólo se describirá esta última. Gracias al texto de ayuda incluido en el módulo SCPM de YaST, el manejo de éste es muy sencillo. Las pocas particularidades del módulo YaST se mencionan en el lugar apropiado.

La documentación actual se encuentra en la sección SCPM de las páginas de información. Estas se pueden consultar con herramientas como Konqueror o Emacs (konqueror info:scpm). En la consola se puede usar `info` o `pinfo`. La información técnica para aquellos que quieran meter las manos en SCPM está en `/usr/share/doc/packages/scpm`.

Si escribes `scpm` sin más argumentos aparecerá un resumen del comando.

Configurar SCPM

Antes de poder trabajar con SCPM, hay que iniciarlo. De manera estándar, SCPM engloba la configuración de redes e impresoras así como la configuración de XFree86 y algunos servicios de red. Si además desea administrar servicios o archivos de configuración, debe activar también los grupos de recursos correspondientes. Puede ver una lista de los grupos de recursos ya definidos con el comando `scpm list_groups`. Si sólo quiere ver los grupos activos, introduzca `scpm list_groups -a`. Todos los comandos deben ser ejecutados por *root*. Para activar o desactivar grupos puede utilizar `scpm activate_group NAME` o bien `scpm deactivate_group NAME`, debiendo sustituir *NAME* por el auténtico nombre de grupo. Otra posibilidad consiste en configurar cómodamente los grupos de recursos mediante el gestor de perfiles de YaST.

Con `scpm enable` se arranca SCPM. La primera vez que se inicia tarda unos segundos. Con `scpm disable` se puede apagar SCPM en cualquier momento, para evitar el cambio no intencionado de perfiles. SCMP continuará iniciándose en los arranques posteriores del sistema.

Crear y administrar perfiles

Al encender SCPM, ya existe un perfil denominado `default` (por defecto). El comando `scpm list` le ofrece una lista de los perfiles disponibles. Este único perfil es por fuerza el perfil activo, lo que se puede ver con `scpm active`. El perfil `default` está pensado como configuración básica, de la cual se derivarán el resto de los perfiles. Por ello primero se deben realizar todas las configuraciones que aparezcan en todos los perfiles. `scpm reload` guarda las modificaciones en el perfil activo. Puede utilizar, renombrar o eliminar el perfil `default`.

Hay dos maneras de crear un perfil. Si el nuevo perfil (aquí con el nombre `work`) p. ej. debe partir del perfil `default`, escriba `scpm copy default work`. A continuación escriba `scpm switch work` para cambiar al nuevo perfil y configurarlo. Pero a veces ya se ha modificado la configuración del sistema para unos determinados fines y éstas se quieren guardar en un nuevo perfil; para esto escriba `scpm add work`.

Ahora la configuración actual del sistema ha quedado guardada en el perfil `work`, que se marcará como activo; esto es, `scpm reload` guarda los cambios en el perfil `work`.

Por supuesto que se puede renombrar o eliminar perfiles. Para ello están los comandos `scpm rename x y` y `scpm delete x`. Para renombrar p. ej. `work` como `trabajo` y eliminarlo posteriormente, escriba

`scpm rename work trabajo` y luego `scpm delete trabajo`. Sólo se eliminará el perfil activo.

De nuevo los comandos por separado:

`scpm list` muestra todos los perfiles disponibles

`scpm active` muestra el perfil activo

`scpm add <nombre>` guarda la configuración actual del sistema en un perfil nuevo y lo vuelve activo

`scpm copy <nombreorigen> <nombredestino>` copia un perfil

`scpm rename <nombreorigen> <nombredestino>` renombra un perfil

`scpm delete <nombre>` elimina un perfil

Indicaciones sobre el módulo YoST: Aquí sólo existe el botón 'Add', lo que puede originar la pregunta de si es posible copiar un perfil existente o guardar la configuración actual. Para renombrar utilice el botón 'Edit'.

Cambiar de un perfil a otro

Para cambiar a otro perfil (aquí llamado `work`) escriba el comando `scpm switch work`. Es lícito cambiar al perfil activo para guardar las opciones modificadas de la configuración del sistema. De forma alternativa, se puede utilizar el comando `scpm reload`.

Para comprender mejor el proceso de cambio entre perfiles y las preguntas que esto pueda causar, se lo explicaremos con un poco más de detalle.

Primero, SCPM comprueba los recursos del perfil activo que fueron modificados desde el último cambio de un perfil a otro. La lista de grupos modificados se genera a partir de la lista de recursos cambiados. A continuación se pregunta para cada uno de estos grupos si los cambios realizados deben guardarse en el perfil activo. Si en lugar de los grupos prefiere ver la lista de recursos individuales como era el caso en las versiones anteriores de SCPM, ejecute el comando `switch` con el parámetro `-r`: `scpm switch -r work`.

Después SCPM compara la configuración actual del sistema con el perfil nuevo al que se quiere cambiar. En este proceso se averiguará qué servicios del sistema se deben conservar o (re)iniciar debido a las modificaciones realizadas en la configuración o a las dependencias mutuas. Nos podríamos imaginar esto como un reinicio parcial del sistema que sólo afecta a una pequeña parte del sistema mientras que el resto sigue trabajando.

A continuación se llevan a cabo las siguientes acciones:

1. Se detienen los servicios del sistema.
2. Se escriben todos los recursos modificados (p. ej. los archivos de configuración).
3. Se (re)inician los servicios del sistema.

Configuración avanzada del perfil

Para cada perfil puede dar una descripción que aparezca con `scpm list`. Para dar una descripción para el perfil activo utilice el comando `scpm set description "texto"`. Para perfiles no activos, debe dar además el nombre del perfil: `scpm set description "texto" work`. A veces ocurre que, al cambiar de un perfil a otro, se ejecutan acciones que (aún) no están previstas en SCPM. Por eso se puede añadir a cada perfil cuatro programas ejecutables o scripts que se ejecuten en distintos momentos del proceso de cambio de un perfil a otro. Estos momentos son:

prestop antes de la parada de los servicios al abandonar un perfil

poststop después de la parada de los servicios al abandonar un perfil

prestart antes del inicio de servicios al activar un perfil

poststart después del inicio de servicios al activar un perfil

El cambio del perfil `work` al perfil `home` transcurre de la siguiente forma:

1. Se ejecuta la acción `prestop` del Perfil `work`.
2. Parada de servicios.
3. Se ejecuta la acción `poststop` del Perfil `work`.
4. Cambio de la configuración del sistema.
5. Se ejecuta la acción `prestart` del perfil `home`.
6. Inicio de los servicios.
7. Se ejecuta la acción `poststart` del perfil `home`.

Con el comando `set` también se pueden añadir estas acciones, y más concretamente, con los comandos `scpm set prestop <nombrearchivo>`, `scpm set poststop <nombrearchivo>`, `scpm set prestart <nombrearchivo>` o `scpm set poststart <nombrearchivo>`. Se debe tratar de un programa ejecutable, es decir, los scripts deben incluir los intérpretes adecuados y al menos poder ser ejecutados por el superusuario (`root`).

Se puede preguntar por las configuraciones añadidas con `set` mediante el comando `get`. Por ejemplo `scpm get poststart` ofrece el nombre del programa `poststart` o nada si no se ha añadido ningún programa. Se puede eliminar estas configuraciones con `""`; esto es, `scpm set prestop ""` retira el programa `poststop`.

Al igual que al incluir la descripción, se puede utilizar todos los comandos `set` y `get` para cualquier perfil. Para ello se añadirá al final el nombre del perfil. Por ejemplo `scpm get prestop <nombrearchivo> work` o `scpm get prestop work`.

Aviso

Puesto que se pueden ejecutar estos scripts o programas con permisos de superusuario, no deberían poder ser modificados por cualquier usuario. Puesto que los scripts pueden contener información confidencial, se recomienda que el superusuario sea el único que los pueda leer. Lo mejor es que proteja estos programas con los permisos

```
-rwx---- root root.
```

```
(chmod 700 <nombrearchivo>    y
chown root:root <nombrearchivo>)
```

Aviso

Selección de perfiles al arrancar

Se puede escoger un perfil nada más arrancar. Para ello sólo se debe introducir el parámetro de arranque `PROFILE=<nombre del perfil>` en el cursor de arranque.

En la configuración del cargador de arranque (`/boot/grub/menu.lst`) también se utiliza el nombre del perfil para la opción `title`. GRUB es el cargador de arranque predeterminado. Puede encontrar abundante información sobre este cargador de arranque en la sección [El arranque con GRUB](#) en la página 77 o bien introduciendo el comando `info grub`. La configuración de GRUB podría ser por ejemplo la siguiente:

```

gfxmenu (hd0,5)/boot/message
color white/green black/light-gray
default 0
timeout 8

title work
    kernel (hd0,5)/boot/vmlinuz root=/dev/hda6 PROFILE=work
    initrd (hd0,5)/boot/initrd

title home
    kernel (hd0,5)/boot/vmlinuz root=/dev/hda6 PROFILE=home
    initrd (hd0,5)/boot/initrd

title road
    kernel (hd0,5)/boot/vmlinuz root=/dev/hda6 PROFILE=road
    initrd (hd0,5)/boot/initrd

```

***Fichero 20:** El archivo /boot/grub/menu.lst*

Para sistemas que todavía utilizan el cargador de arranque LILO, puede tomarse como ejemplo el archivo [21](#).

```

boot      = /dev/hda
change-rules
reset
read-only
menu-scheme = Wg:kw:Wg:Wg
prompt
timeout = 80
message = /boot/message

    image = /boot/vmlinuz
    label = home
    root = /dev/hda6
    initrd = /boot/initrd
    append = "vga=0x317 hde=ide-scsi PROFILE=home"

    image = /boot/vmlinuz
    label = work
    root = /dev/hda6
    initrd = /boot/initrd
    append = "vga=0x317 hde=ide-scsi PROFILE=work"

    image = /boot/vmlinuz

```



```
label = road
root = /dev/hda6
initrd = /boot/initrd
append = "vga=0x317 hde=ide-scsi PROFILE=road"
```

Fichero 21: Archivo /etc/lilo.conf

Ahora al arrancar se puede seleccionar fácilmente el perfil deseado.

Problemas y soluciones

Por regla general, SCPM debería funcionar sin problemas. No obstante, existen algunos casos problemáticos que se describen a continuación.

Hasta el momento de escribir estas líneas, SCPM todavía no es capaz de administrar una actualización del sistema. El principal problema radica en que los datos almacenados en los distintos perfiles no pueden ser actualizados por los mecanismos de actualización. SCPM detecta que se ha realizado una actualización y se niega a prestar sus servicios. El usuario obtiene un mensaje de error de SCPM informando de que la instalación del sistema se ha modificado o es desconocida. En este caso, la solución consiste en reiniciar SCPM con `scpm -f enbale`. Sin embargo, al realizar esta acción los perfiles se pierden y deben ser configurados de nuevo.

En algunos casos, SCPM se interrumpe de forma repentina durante un proceso de switch o cambio de perfil. La causa puede provenir del exterior (proceso terminado por el usuario, batería del portátil vacía, etc.) o bien puede tratarse de un fallo interno de SCPM. Al intentar reiniciar SCPM, obtendrá un mensaje de error diciendo que SCPM está bloqueado. El objeto de este bloqueo es proteger el sistema, ya que los datos guardados en la base de datos de SCPM pueden no coincidir con el estado actual de su sistema. En este caso, borre simplemente el archivo de bloqueo con el comando `rm /var/lib/scpm/#LOCK` y recargue SCPM con `scpm -s reload` para que el sistema vuelva a ser coherente. A continuación ya puede trabajar como de costumbre.

Una última indicación: Normalmente no supone ningún problema el modificar la configuración de un grupo de recursos una vez que ya se ha iniciado SCPM. Lo único que debe tener en cuenta es ejecutar `scpm rebuild` cuando haya terminado de añadir o eliminar grupos. Este comando se encarga de añadir nuevos recursos a todos los perfiles y eliminar los recursos borrados. No obstante, estos recursos no se eliminan definitivamente hasta que no los configura de forma distinta en los diversos perfiles, momento en el que pierde estos datos de configuración (excepto la versión actual de los datos en su sistema, la cual no es

modificada por SCPM). Si edita la configuración con YqST no es necesario que ejecute ningún comando rebuild; YqST se ocupa de ello automáticamente.

APM y ACPI – Powermanagement

El sistema de control de energía (ingl. *powermanagement*) requiere un hardware y una rutina de la BIOS apropiados. La mayoría de los ordenadores portátiles y muchos ordenadores de sobremesa cumplen estos requisitos. Hasta ahora se utilizó principalmente el estándar APM (Advanced Power Management). Básicamente se trata de funciones implementadas en la BIOS del ordenador. Por esta razón el control de energía no funcionaba igual de bien con todos los dispositivos. Si tiene un portátil con una implementación APM en funcionamiento, hace bien en utilizarla. Sin embargo, desde hace un tiempo, algunos fabricantes quieren dejar de lado APM y pasar a utilizar totalmente el nuevo estándar ACPI (Advanced Configuration and Power Interface). Pero ACPI es más complicado y requiere una buena colaboración entre fabricantes de hardware, programadores de BIOS y expertos del sistema operativo. Además la implementación ACPI en el kernel de Linux aún no está acabada, por lo que sólo se puede utilizar parcialmente. Con el kernel 2.6 se espera una mejora sustancial.

Funciones para el ahorro de energía

Muchas de estas funciones son de interés general, pero sólo llegan a ser realmente importantes cuando se trata de ordenadores portátiles. A continuación se describen estas funciones y se explica en qué sistema se pueden llevar a cabo.

En reposo (ingl. *stand-by*) Sólo se desactiva la pantalla y en algunos dispositivos se reduce también el rendimiento del procesador. No todos los APM tienen disponible esta función. En ACPI este estado se corresponde con S1.

Suspensión (a memoria) Para este modo toda la información sobre el estado del sistema se guarda en la memoria y, aparte de esta, todo el resto del sistema se para. Es un estado en el cual el ordenador gasta muy poca energía, así que se puede pasar desde 12 horas hasta varios días con la batería. La gran ventaja es la de volver dentro de pocos segundos al estado anterior de trabajo, sin necesidad de arrancar y cargar de nuevo los programas usados. El atractivo especial de realizar esto con Linux es el no tener que parar el ordenador nunca; hay otros sistemas operativos que se vuelven inestables después de cierto tiempo. En la mayoría de los

portátiles actuales basta con cerrar la tapa para suspender y abrirla después para seguir trabajando. En ACPI este estado se corresponde con S3.

Hibernación (suspensión a disco) En este modo el ordenador aguanta todo el invierno (Hibernation == Invernar), ya que todo el contenido de la memoria se “vuelca” al disco duro y el sistema se para después. El ordenador tarda de 30 a 90 segundos y también se restablece por completo el estado anterior. Algunos fabricantes ofrecen ciertos modos híbridos (p. ej. RediSafe en IBM Thinkpads). En ACPI el estado de hibernación se corresponde con S4.

Para Linux también existe una gran cantidad de soluciones de software que sin embargo no se incluyen en SuSE Linux. Si quiere utilizarlas:

<http://falcon.sch.bme.hu/~seasons/linux/swsusp.html>

Control de batería Junto a la información del estado de la batería también es importante tener algo previsto en caso de que disminuyan las reservas de energía. La mayor parte de las veces las rutinas APM de la BIOS se encargan de ello. De forma alternativa, se puede utilizar los comandos `apmd/acpid` o `klaptopdaemon`.

Apagado automático Después de un “Shutdown” el ordenador se para completamente sin necesidad de pulsar el botón de apagar. Esto es importante en caso de que se realice un apagado automático poco antes de que se vacíe la batería.

Apagado de los componentes del sistema Los componentes esenciales a la hora de ahorrar energía son los discos duros. Dependiendo de la fiabilidad, se puede “poner a dormir” el sistema durante más o menos tiempo. El riesgo de una pérdida de datos se incrementa con la duración del período de reposo de los discos. Se puede desactivar otros componentes via ACPI (al menos en teoría) o de forma duradera en el setup de la BIOS. Ante todo el puerto de infrarrojos debería permanecer apagado siempre que no se esté utilizando (véase la sección *IrDA – Infrared Data Association* en la página 244).

Control del rendimiento del procesador Junto con APM suele existir la posibilidad de escoger distintas configuraciones en el setup de la BIOS. Para algunos dispositivos existen herramientas especiales para controlar este tipo de opciones de configuración. Por ejemplo, para los Thinkpads de IBM se encuentran `tpctl` y `apmiser` del paquete `package tpctl`. El programa `procspeed` del paquete `apmd` permite controlar la frecuencia del procesador. Sólo es posible influir directamente en el rendimiento del procesador por medio de ACPI. Por este motivo, esta posibilidad se explica posteriormente en el apartado sobre ACPI.

APM

Algunas de las funciones de ahorro de energía las realiza sólo el APM de la BIOS. El estado de reposo y el de suspensión se pueden activar con una combinación de teclas o cerrando la tapa en la mayoría de los ordenadores portátiles. Estos modos de operación se realizan sin intervención del sistema operativo. Para iniciarlos mediante un comando o si hace falta ejecutar ciertas acciones antes de suspender, hay que instalar determinados paquetes y un kernel adecuado.

El soporte APM forma parte integral de los kernels de SuSE Linux, pero sólo se activa si en la BIOS no se ha implementado ACPI y si se encuentra un APM-BIOS. Para activar el soporte APM, ACPI ha desactivarse en el prompt de arranque con `acpi=off`. Puede comprobar si APM ha sido activado ejecutando el comando `cat /proc/apm`. Si aparece una línea con diversos números, todo está en orden. A continuación deberá apagar el ordenador con el comando `shutdown -h`.

Algunas BIOS no cumplen el estándar APM al cien por cien, por lo que puede aparecer un comportamiento "extraño". Algunos problemas se pueden resolver con parámetros especiales (antiguamente eran opciones de configuración del kernel). Todos los parámetros se introducen en un prompt de arranque con la forma `apm=<parameter>`:

on/off Activar o desactivar el soporte APM.

(no-)allow-ints Permitir interrupciones durante la ejecución de funciones de la BIOS.

(no-)broken-psr La BIOS tiene una función arruinada "GetPowerStatus"

(no-)realmode-power-off Reducir la velocidad del procesador antes del apagado

(no-)debug Registrar acontecimientos APM en Syslog

(no-)power-off Desconectar todo el sistema tras el apagado

bounce-interval=<n> Tiempo en 1/100 segundos, durante el cual se deben pasar por alto otros acontecimientos de suspensión tras haberse producido el primero

idle-threshold=<n> Porcentaje de la actividad del sistema, a partir del cual la función de la BIOS se volverá inactiva (0=siempre, 100=nunca)

idle-period=<n> Tiempo en 1/100 segundos, por encima del cual se deducirá la actividad o inactividad del sistema

El daemon APM (apmd)

El daemon `apmd` controla el estado de la batería y es capaz de iniciar ciertas actividades cuando se pone el ordenador en estado de “reposo” o “suspensión”. Se encuentra en el paquete `apmd` y, aunque no es imprescindible para trabajar, sí resulta muy útil.

El `apmd` no se inicia automáticamente en el arranque. Pero si se requiere, se puede cambiar la configuración de los servicios del sistema con el módulo de niveles de ejecución de `YAST`. De forma alternativa se puede emplear el programa `chkconfig`. Para iniciarlo manualmente utilice `rcapmd start`.

El daemon se configura mediante algunas variables que se encuentran en `/etc/sysconfig/powermanagement`. Este archivo ya contiene comentarios por lo que a continuación sólo se dan algunas indicaciones.

APMD_ADJUST_DISK_PERF De esta forma se puede determinar que el comportamiento del disco duro se adapte al suministro de energía. Para esto hay una gran cantidad de variables que comienzan con `APMD_BATTERY` o con `APMD_AC`. La primera contiene las opciones de la batería; la última, el funcionamiento de la fuente de alimentación externa.

APMD_BATTERY/AC_DISK_TIMEOUT Indica el tiempo que durará la inactividad del disco. Los valores se encuentran en el apartado *Parar el disco duro* en la página 243 o en las páginas man con `hdparm` con la opción `-S`

APMD_BATTERY/AC_KUPDATED_INTERVAL El tiempo que debe transcurrir entre dos acciones del Kernel Update Daemon.

APMD_BATTERY/AC_DATA_TIMEOUT La edad máxima de los datos en el búfer.

APMD_BATTERY/AC_FILL_LEVEL La capacidad máxima del búfer del disco duro

APMD_PCMCIA_EJECT_ON_SUSPEND Aunque para SuSE Linux se compila PCMCIA con soporte APM, a veces surgen problemas. Algunos controladores de tarjetas PCMCIA no vuelven a un estado correcto después de suspender el sistema (p. ej. `xirc2ps_cs`). Por eso el `apmd` es capaz de desactivar el sistema PCMCIA antes de suspender el sistema y después activarlo nuevamente. Para realizar esta característica, la variable `APMD_PCMCIA_EJECT_ON_SUSPEND` debe estar en `yes`.

APMD_INTERFACES_TO_STOP Aquí se pueden indicar interfaces de red que deben ser apagadas antes de suspender el sistema y reiniciadas después.

APMD_INTERFACES_TO_UNLOAD Si además hay que descargar el módulo de las interfaces, utilice esta variable.

APMD_TURN_OFF_IDEDMA_BEFORE_SUSPEND A veces no funciona el sistema – no vuelve a reactivarse después de una suspensión –, si un dispositivo IDE (disco duro) aún se encuentra en modo DMA.

Existen más posibilidades, como p. ej. el tiempo de repetición del teclado o la hora, que se deben corregir tras una suspensión o un apagado automático del portátil, al enviar el APM de la BIOS un acontecimiento de "estado crítico de la batería". Para los usuarios avanzados queda la posibilidad de añadir funcionalidades al archivo `/usr/sbin/apmd_proxy`, que lleva a cabo las acciones mencionadas arriba.

Comandos adicionales

`apmd` contiene algunas utilidades adicionales. `apm` indica la capacidad actual de la batería y pone el sistema en "reposo" (`apm -S`) o "suspendido" (`apm -s`); ver página del manual de `apm` (`man apm`).

Con el comando `apmsleep` se puede suspender el sistema por un tiempo determinado; ver `apmsleep`.

Para visualizar un archivo log sin necesidad de mantener el disco duro girando, se puede usar `tailf` como reemplazo de `tail -f`.

También hay herramientas para sistema X Window como p. ej. `xapm apmd` que indica de forma gráfica la carga de la batería. Usando el entorno KDE, o al menos `kpanel`, se puede visualizar con `kbatmon` el estado de carga de la batería y suspender el sistema. Como alternativa también es interesante `xosview`.

ACPI

Información general

ACPI significa (ingl. *Advanced Configuration and Power Interface*). La función de ACPI es permitir al sistema operativo configurar y controlar cada componente de hardware por separado. De este modo, ACPI sustituye tanto a Plug and Play como a APM. En este capítulo no se tratará la parte de ACPI que se encarga de iniciar el hardware (donde apenas interviene el usuario).

La BIOS dispone de tablas donde se recoge información sobre cada componente y sobre los métodos para acceder al hardware. El sistema operativo utiliza esta información, por ejemplo, para asignar Interrupts o para activar y desactivar componentes de hardware.

No obstante, debido a que el sistema operativo sigue las instrucciones almacenadas en la BIOS, aquí también se está supeditado a la implementación de la BIOS. Los mensajes producidos durante el arranque se almacenan en `/var/log/boot.msg`. Allí, ACPI informa de qué tablas ha encontrado y evaluado con éxito.

DSDT Differentiated System Description Table: Contiene información sobre los componentes del ordenador y cómo se pueden configurar dichos componentes.

FADT Fixed ACPI Description Table: Contiene información sobre la implementación del bloque de registro para el hardware ACPI además de la dirección física de DSDT.

MADT Multiple APIC Description Table: Describe la implementación y configuración de APIC.

RSDT Root System Description Table: Tabla de indicadores al resto de tablas. El indicador a RSDT (RSDP) debe encontrarse en la zona baja de la memoria.

SSDT Secondary System Description Table: Esta tabla es una continuación de DSDT. Puede haber varias SSDT. La distribución entre varias tablas aumenta la flexibilidad, sobre todo para OEM.

XSDT Extended Root System Description Table: Contiene la misma información que la tabla RSDT, pero puede incluir indicadores mayores de 32 bits en la cabecera de descripción. Por su parte, la tabla RSDP puede hacer referencia a la XSDT.

El estándar ACPI define una variedad de estados en los que se puede encontrar el sistema. En primer lugar se encuentran los estados principales:

G0 El sistema está trabajando.

G1 El sistema duerme, cambio a G0 sin arrancar el sistema operativo (suspend).

G2 Soft off, el sistema operativo debe arrancar al encender el ordenador.

G3 Interruptor apagado, el sistema no tiene electricidad (el interruptor principal está apagado)

Además hay 6 estados de sueño con los que se puede diferenciar aún más entre G0/G1/G2:

S0 El sistema está trabajando.

S 1 Stand-by (reducido consumo de energía, vuelve a "despertarse" muy rápidamente).

S2 Otra modalidad de stand-by que no suele estar implementada en los dispositivos.

S3 Suspend (consumo mínimo de energía, vuelve a "despertarse" muy rápidamente).

S4 Hibernation o Suspend To Disk (ningún consumo de energía, tarda un poco más en "despertarse" (de 20a 100 segundos dependiendo del hardware))

S5 Soft off (G2)

A éstos se suman los estados D0 - D3, en los que cada componente de hardware está activo, en suspenso, o apagado. Solamente el procesador conoce aún más estados para circunstancias especiales de funcionamiento. Los estados C son activados por comandos del CPU sobre los que el usuario no puede influir directamente:

C0 El procesador está trabajando.

C1 El procesador ejecuta instrucciones especiales para interrupciones que, precisando poca energía, permiten reanudar el trabajo muy rápidamente.

C2 Como C1, sólo que con un consumo de energía aún más bajo y mayor tiempo requerido para reanudar el trabajo.

C3 Como C2, sólo que con mayor ahorro de energía. El caché de primer nivel tendrá inconsistencias. (Implementado sólo en algunos dispositivos y de uso muy poco extendido).

Los estados en cuanto a potencia dependen de técnicas especiales para el procesador como Speedstep (Intel) o PowerNow (AMD), en las que se modifica la frecuencia de reloj y la tensión del núcleo del CPU.

P0 Máxima frecuencia de reloj y tensión del núcleo

P1 Primer nivel de ahorro, se reducen la frecuencia y la tensión

P2 Siguiente nivel de ahorro (si está disponible)

P3 ...

La tercera posibilidad de ahorro de energía en el procesador es el throttling, que consiste en interrumpir periódicamente la señal de reloj del procesador.

T0 0 % desconexión del reloj

T1 12 % desconexión del reloj

T2 25 % desconexión del reloj

T4 ...

Los estados P y T pueden ser activados directamente por el usuario (o un daemon). La principal diferencia radica en el ahorro de energía. El throttling permite tan sólo un ahorro lineal, es decir, 25 % de desconexión del reloj se traduce en 25 % menos de rendimiento con un ahorro de energía del 25 % (sólo del procesador). En cambio, si se modifica la potencia, la cantidad de energía que se ahorra es mayor que el rendimiento que se pierde gracias a la menor tensión del núcleo. La disminución de rendimiento se utiliza también como "enfriamiento pasivo" en contraposición al enfriamiento activo mediante ventiladores. Además puede resultar de utilidad si se quiere recargar las baterías más rápidamente mientras se usa el ordenador.

ACPI recoge información sobre las baterías, el adaptador de red, la temperatura y los ventiladores, e informa sobre eventos del sistema como bajar la cubierta o poca carga en la batería.

ACPI en la práctica

Cuando el kernel reconoce una BIOS ACPI durante el arranque, ACPI es activado automáticamente (y APM desactivado). El parámetro de arranque `acpi=on` podría ser necesario, como máximo, en máquinas antiguas. No obstante, el ordenador tiene que soportar ACPI 2.0 o superior. Para comprobar si ACPI está activado, consulte los mensajes de arranque del kernel en `/var/log/boot.msg`. También existe un directorio `/proc/acpi` que se explicará más adelante.

A continuación es necesario cargar una serie de módulos para el OSPM ("Operating System Power Management"), de lo que se ocupa el script de inicio del daemon ACPI. Si alguno de estos módulos causa problemas, puede impedirse su carga o descarga en `/etc/sysconfig/powermanagement`. En el registro del sistema (`/var/log/messages`) se encuentran los mensajes del módulo y puede observarse qué componentes han sido detectados.

En `/proc/acpi` aparecen ahora varios archivos que informan sobre el estado del sistema o permiten modificar de forma activa algunos de estos estados. No

obstante, esta funcionalidad no es ni mucho menos completa porque, o bien está todavía en desarrollo, o bien depende de lo que haya implementado el fabricante. La mayor limitación:

Aviso

El modo en suspenso todavía no funciona con ACPI: ni `suspend to RAM` ni `to disk` (hibernation). Por motivos internos del kernel, estas funciones estarán disponibles para el kernel 2.6 (ó 2.5 para los mañosos). Los más valientes pueden integrar el parche `sw-susp` en el kernel. Véanse las funciones de ahorro de energía: hibernation.

Aviso

Se puede leer todos los archivos (excepto `dsdt` y `fadt`) con `cat`. En algunos se puede incluso modificar opciones pasando a `X` valores adecuados con `echo X > archivo`. (Todo lo que se encuentra en `/proc` no son archivos en el disco duro sino más bien una interfaz al kernel). A continuación se describen los archivos más importantes:

`/proc/acpi/info` Información general sobre ACPI

`/proc/acpi/alarm` Aquí puede definirse cuándo el sistema "despierta" de un estado de sueño. La hora se indica mediante `echo año-mes-día hora:minutos:segundos > /proc/acpi/alarm`. Pero puesto que los estados de sueño actualmente no funcionan, no tiene mucho sentido poner el "despertador".

`/proc/acpi/sleep` Proporciona información sobre los posibles estados de sueño. Aquí se podrá provocar un estado `suspend` próximamente. En la actualidad funcionan como máximo `S1` (stand-by) y `S5` (no se recomienda porque el sistema no se apaga correctamente): `echo 1 > /proc/acpi/sleep`.

`/proc/acpi/event` Aquí se registran los eventos del sistema. Éstos son procesados por daemons como `'acpid'` o `'ospm'`. Si no interviene ningún daemon, los eventos se pueden leer con `'cat /proc/acpi/event'` (salir con Ctrl-C). Un ejemplo de evento es pulsar el interruptor principal o cerrar la cubierta del portátil.

`/proc/acpi/dsdt` y `/proc/acpi/fadt` Aquí se almacenan las tablas ACPI DSDT y FADT. Éstas pueden leerse con `acpidmp`, `acpidisasm` y `dmdecode`.
Puede encontrar estos programas junto con la correspondiente documentación en paquete `pmtools`. Por ejemplo:
`acpidmp DSDT | acpidisasm`.

`/proc/acpi/ac_adapter/AC/state` ¿Está conectado el adaptador de red?

/proc/acpi/battery/BAT*/{alarm,info,state} Contienen abundante información sobre el estado de la batería. Para comprobar el nivel de carga es necesario comparar `last full capacity` de `info` con `remaining capacity` de `state`. Aunque esto también puede hacerse más fácilmente con la ayuda de programas especiales que se describirán más adelante. En `alarm` se puede introducir qué cantidad de carga provocará un evento en la batería.

/proc/acpi/button Este directorio contiene información sobre diversos botones.

/proc/acpi/fan/FAN/state Muestra si el ventilador está funcionando en ese momento. También puede encenderse o apagarse manualmente escribiendo en el archivo 0 (=encender) ó 3 (=apagar). No obstante, hay que tener en cuenta que tanto el código ACPI del kernel como el hardware (o la BIOS) sobrescriben estos valores cuando la temperatura es demasiado elevada.

/proc/acpi/processor/CPU0/info Información sobre las posibilidades de ahorro de energía del procesador.

/proc/acpi/processor/CPU0/power Información sobre el estado actual del procesador. Un asterisco en C2 significa inactividad y es el estado más frecuente, como puede apreciarse en el número `usage`.

/proc/acpi/processor/CPU0/performance Esta interfaz ya no se utiliza. Véase al respecto el apartado *Speedstep o PowerNow* en la página siguiente.

/proc/acpi/processor/CPU0/throttling Permite aumentar de forma lineal el ahorro de energía del procesador.

/proc/acpi/processor/CPU0/limit Si un daemon se encarga de regular automáticamente la potencia y el throttling, aquí se pueden definir los límites que no se deben sobrepasar en ningún caso. Existen límites fijados por el sistema y uno que puede ser definido por el usuario. Con `echo 1:5 > /proc/acpi/processor/CPU0/limit` se consigue que los estados P0 ó T0-T4 nunca sean utilizados.

/proc/acpi/thermal_zone/ Aquí se encuentra un subdirectorio para cada zona térmica. Una zona térmica es una sección con características térmicas semejantes, cuyo número y nombre de fabricante de hardware puede ser seleccionado. Muchas de las posibilidades ofrecidas por ACPI se implementan rara vez. En su lugar, la BIOS se ocupa normalmente de controlar la temperatura sin que el sistema operativo intervenga, ya que aquí se trata nada menos que de la duración del hardware. Por lo tanto, las descripciones siguientes son en parte puramente teóricas.

/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 "activa" o "pasiva". En los casos donde el control del ventilador no depende de ACPI, el estado es siempre "ok".

/proc/acpi/thermal_zone/*/cooling_mode Bajo un control total por parte de ACPI, aquí se puede seleccionar el método de refrigeración preferido: pasivo (menor rendimiento pero mayor ahorro) o activo (siempre máximo rendimiento pero con el ruido del ventilador a toda potencia).

/proc/acpi/thermal_zone/*/trip_points Aquí se puede definir la temperatura a partir de la cual se emprende alguna acción. Esta acción puede abarcar desde la refrigeración activa o pasiva hasta apagar el ordenador ("critical"), pasando por suspend ("hot").

/proc/acpi/thermal_zone/*/polling_frequency Si el valor de "temperature" no se actualiza automáticamente cuando se modifica la temperatura, se puede cambiar aquí al modo "polling". El comando `echo X > /proc/acpi/thermal_zone/*/polling_frequency` hace que cada X segundos se pregunte la temperatura. El modo "polling" se desconecta con X=0.

El daemon ACPI (acpid)

De forma semejante al daemon APM, el daemon ACPI procesa determinados eventos ACPI, tales como los que activan el encendido y apagado o el contacto de la tapa. Todos los acontecimientos quedan registrados en el log del sistema. En `/etc/sysconfig/powermanagement` con las variables `ACPI_BUTTON_POWER` y `ACPI_BUTTON_LID` se puede establecer qué debe ocurrir en esos acontecimientos. Si no es suficiente, puede adaptar el script `/usr/sbin/acpid_proxy` o cambiar la configuración de `acpid` en `/etc/acpi/`.

Al contrario que en `apmd`, aquí no hay muchas opciones preconfiguradas ya que ACPI para Linux está todavía en pleno desarrollo. Dado el caso, es necesario configurar `acpid` por sí mismo.

Speedstep o PowerNow

Los procesadores de dispositivos móviles tienen la posibilidad de ajustar la frecuencia del procesador a las condiciones actuales del sistema. La interfaz de esta tecnología ha sido trasladada a ACPI. Las frecuencias posibles se encuentran

en `/proc/cpufreq` y `/proc/sys/cpu/0/speed*`, donde también puede configurarse la frecuencia actual. Puede encontrar información adicional en `/usr/src/linux/Documentation/cpufreq/`.

El daemon `cpufreqd` se encarga de ajustar automáticamente la frecuencia del procesador a los requisitos actuales del sistema. No obstante, este daemon no se inicia automáticamente al arrancar el sistema. Puede obtener más información sobre el inicio de servicios del sistema en la sección *El editor de niveles de ejecución de YaST* en la página 303. La documentación de `cpufreqd` se encuentra en `/usr/share/doc/packages/cpufreqd/README.SuSE` y en la página del manual `man cpufreqd`. La configuración se lleva a cabo en `/etc/sysconfig/powermanagement`.

Otras herramientas

Existe una serie de herramientas ACPI más o menos completas. Entre ellas se encuentran herramientas puramente informativas que muestran el estado de la batería o la temperatura (`acpi`, `klaptopdaemon`, `wmacpimon`, etc.). Otras facilitan el acceso a las estructuras bajo `/proc/acpi` o ayudan a observar cambios (`akpi`, `kacpi`, `gtkacpiw`), y otras permiten editar las tablas ACPI en la BIOS (paquete `pmtools`).

Posibles problemas y soluciones

Se puede distinguir entre dos tipos de problemas. Por una parte, puede haber fallos en el código ACPI del kernel que no se han detectado a tiempo. En este caso se proporcionará una solución para descargar. Otros problemas más incómodos y, por desgracia, también más frecuentes, son los problemas en la BIOS del ordenador. Se da incluso el caso de que se integran en la BIOS desviaciones de las especificaciones ACPI para evitar fallos en la implementación ACPI en otros sistemas operativos de uso extendido. Existe también hardware en el que se conocen fallos graves en la implementación ACPI. Por este motivo, estos componentes de hardware se incluyen en una lista negra para que el kernel de Linux no utilice en ellos ACPI.

En caso de problemas, en primer lugar se debe actualizar la BIOS, lo que funciona con éxito en muchas ocasiones. Si el ordenador ni siquiera arranca correctamente, pruebe a utilizar algunos de los siguientes parámetros de arranque:

pci=noacpi No utilizar ACPI para configurar los dispositivos PCI.

acpi=oldboot Ejecutar sólo recursos simples de configuración, en caso contrario no utilizar ACPI.

acpi=off No utilizar ACPI en absoluto.

Es muy importante examinar los mensajes de arranque cuidadosamente. Para ello lo mejor es utilizar el comando `dmesg | grep -2i acpi` después del arranque (o incluso examinar todos los mensajes, ya que el problema no debe radicar necesariamente en ACPI). Si ocurre un error durante el análisis sintáctico de una tabla ACPI, existe la posibilidad (al menos para la tabla más importante, DSDT) de integrar una tabla mejorada en un kernel personalizado. No obstante, esta no es tarea fácil y requiere la ayuda de expertos. Para algunos ordenadores, ya existen en Internet tablas DSDT libres de fallos.

En la configuración del kernel existe un botón para activar los mensajes de depuración de ACPI. Si se ha compilado e instalado un kernel con depuración ACPI, puede ayudar con información detallada a los expertos que busquen un posible fallo.

En cualquier caso, siempre resulta una buena idea ponerse en contacto con el fabricante del aparato si ocurriesen problemas con el hardware o la BIOS. Aún cuando los fabricantes no siempre pueden ayudar cuando se trata de Linux, es importante que escuchen el término Linux lo más a menudo posible. No tomarán a Linux en serio hasta que no se den cuenta de que un número importante de sus clientes lo utilizan. Aunque no tenga ningún problema, tampoco está de más que informe al fabricante de su hardware de que lo usa con Linux.

Puede encontrar ayuda y documentación adicional (en inglés) en:

- http://www.columbia.edu/~ariel/acpi/acpi_howto.txt (how-to ACPI, algo incompleto y poco actual)
- <http://www.cpqlinux.com/acpi-howto.html> (más completo que el anterior, incluye parches para la tabla DSDT)
- <http://www.intel.com/technology/iapc/acpi/faq.htm> (preguntas de uso frecuente sobre ACPI de @Intel)
- <http://acpi.sourceforge.net/> (el proyecto ACPI4Linux en Sourceforge)
- <http://codecs.home.sapo.pt/acpi/index.html> (parches ACPI)
- <http://www.poupinou.org/acpi/> (parches DSDT de Bruno Ducrot)
- <http://sourceforge.net/projects/cpufreqd> (el proyecto CPUFreq en Linux)
- <http://sourceforge.net/projects/swsusp> (hibernación del kernel: proyecto swsusp)
- Lista de correos: lister.fornax.hu/pipermail/swsusp

Parar el disco duro

En Linux es posible parar el disco duro cuando no se necesita. Esto se realiza mediante el programa `hdparm`, que tiene varias opciones. Por ejemplo `-y` pone el disco duro inmediatamente en modo de "reposo", mientras que `-Y` lo para completamente. Con `hdparm -S <x>` se consigue que el disco duro se apague tras un determinado período de inactividad. La posición `<x>` tiene distintos significados: 0 apaga el mecanismo, el disco sigue funcionando; los valores entre 1 y 240 se multiplican por 5 segundos; entre 241 y 251 corresponden desde 1 a 11 veces 30 minutos.

Sin embargo a menudo no es tan sencillo puesto que existe una gran cantidad de procesos en Linux que escriben datos en el disco y lo reactivan una y otra vez. Por tanto es importante comprender la forma en que Linux trabaja con los datos que se deben escribir en el disco.

Primero se envían todos los datos a un búfer que escribe en la memoria de trabajo, el cual es controlado por el 'Kernel Update Daemon' (`kupdated`). Siempre que un dato alcance una determinada "edad" o el búfer se llena hasta un determinado nivel, el búfer se vacía y se pasan los datos al disco duro. El tamaño del búfer es dinámico y depende del tamaño de la memoria y del sistema. Puesto que la prioridad es la seguridad de los datos, el `kupdated` funciona a pequeños intervalos de tiempo: prueba el búfer cada 5 segundos e informa al daemon '`bdflush`' de qué datos llevan más de 30 segundos en el búfer o si este se encuentra lleno al 30 %. Entonces el daemon `bdflush` escribe los datos en el disco, aunque también lo hace independientemente de `kupdated`. Si tiene un sistema estable puede cambiar estas configuraciones, pero no olvide que puede disminuir el nivel de seguridad de sus datos.

Se puede encontrar las configuraciones con `cat /proc/sys/vm/bdflush`. El primer valor es el nivel de llenado del búfer a partir del cual este se vacía. El sexto valor es la edad máxima de los datos en el búfer, contada en 1/100 segundos.

El quinto valor es el intervalo en que `kupdated` prueba el búfer, también en 1/100 segundos. Para p. ej. aumentar el intervalo de `kupdated` a un minuto, introduzca nuevos números en este archivo.

```
echo 30 500 0 0 6000 > /proc/sys/vm/bdflush
```

Así

```
echo 60 > /proc/sys/vm/bdflush
```

cambia el nivel de llenado del búfer al 60 %. El resto de los valores están descritos en el archivo `Documentation/filesystems/proc.txt` de las fuentes del kernel.

Cuidado: Las modificaciones en la configuración del Kernel Update Daemon influyen en la seguridad de los datos. Si no está seguro, no lo haga.

Las opciones del timeout del disco duro, del intervalo kupdated, del nivel de llenado del búfer y de la edad de los datos se pueden depositar dos veces en `/etc/sysconfig/powermanagement`: una para la batería y otra para el funcionamiento del suministro externo de energía. Las variables se describen en el apartado 'apmd' y en el mismo archivo.

Además de todo lo anterior, los denominados "sistema de archivos Journaling", como p. ej. reiserfs o ext3, escriben sus metadatos en el disco duro independientemente de bdflush, lo cual también impide que el disco duro quede inactivo. Para evitarlo se ha desarrollado una ampliación del kernel específica para dispositivos móviles. Esta ampliación se describe en `/usr/src/linux/Documentation/laptop-mode.txt`.

Naturalmente también se debe tener en cuenta la forma en que se comportan los programas que se están utilizando. p. ej. los buenos editores de texto escriben con regularidad los archivos modificados en el disco, lo cual hace que el disco se reactive una y otra vez. Tales propiedades se pueden desactivar pero esto provoca una disminución en el nivel de seguridad de los datos.

IrDA – Infrared Data Association

IrDA ("Infrared Data Association") es un estándar industrial para la comunicación inalámbrica por onda infrarroja. Muchos de los portátiles que se venden hoy en día incorporan un emisor/receptor que permite la comunicación con otros dispositivos tales como impresoras, módems, LAN u otros portátiles. La tasa de transferencia se sitúa entre 2400 bps y 4 Mbps.

Hay dos modos de funcionamiento para IrDA. El modo estándar SIR se comunica con el puerto infrarrojo a través de una conexión serie. Este modo funciona con casi todos los dispositivos y cumple todas las exigencias. El modo más rápido FIR requiere un driver especial para el chip IrDA, pero no existen drivers para todos los chips. Además se debe configurar el modo deseado en el setup de la BIOS. Allí se puede averiguar la conexión serial que se utiliza para el modo SIR.

Puede encontrar información sobre IrDA en el IrDA-Howto de Werner Heuser en <http://tuxmobil.org/Infrared-HOWTO/Infrared-HOWTO.html> y en la página web del Proyecto IrDA de Linux <http://irda.sourceforge.net/>.

Software

Los módulos necesarios se incluyen en el paquete del kernel. El paquete `irda` contiene los programas de ayuda necesarios para el soporte de la conexión de infrarrojos. La documentación al respecto se encuentra después de la instalación en `/usr/share/doc/packages/irda/README`.

Configuración

IrDA no se instala automáticamente al arrancar. Utilice el módulo `Runlevel` de `YaST` para cambiar las configuraciones de este servicio del sistema. Otra opción es utilizar el programa `chkconfig`. Desgraciadamente, IrDA requiere más energía (corriente externa o batería), puesto que envía un paquete `Discovery` cada dos segundos, con el fin de reconocer automáticamente otros dispositivos periféricos. Por esto, si trabaja con batería, debería arrancar IrDA sólo cuando lo vaya a utilizar. Con el comando

```
rcirda start
```

puede activar manualmente la conexión, o desactivarla (con el parámetro `stop`). Al activar la conexión se cargarán automáticamente los módulos del kernel necesarios.

En el fichero `/etc/sysconfig/irda` sólo hay una variable `(IRDA_PORT)`. Allí puede configurar la conexión que se va a utilizar en modo SIR; el script `/etc/irda/drivers` se encarga de esta configuración cuando se inicia el soporte de infrarrojos.

Uso

Para imprimir por vía infrarroja, es posible enviar los datos a través del fichero de dispositivo `/dev/ir_lpt0`. Este se comporta igual que la interfaz o fichero de dispositivo `/dev/lp0` con conexión "alámbrica" sólo que los datos viajan por vía infrarroja.

Se puede configurar una impresora que trabaja con el puerto IrDA tal como una impresora en el puerto paralelo o puerto serie. Al imprimir, asegúrese de que la impresora esté "a la vista" del puerto IrDA del ordenador y de que el soporte de infrarrojos se haya iniciado.

El fichero de dispositivo `/dev/ircomm0` permite comunicarse con otros ordenadores, con teléfonos móviles o con dispositivos similares. Con el programa `wvdial` se puede entrar vía infrarrojos a Internet usando por ejemplo el móvil S25 de Siemens. También es posible comparar datos con la Palm Pilot, para lo

cual sólo tiene que introducir `/dev/ircomm0` como dispositivo en el programa correspondiente.

Tenga en cuenta que sólo se puede comunicar directamente con dispositivos que soportan los protocolos Printer o IrCOMM. Con programas especiales (como `irobexpalm3`, `irobexreceive`, teniendo en cuenta la descripción en IR-HOWTO) también nos puede comunicar con dispositivos que utilizan el protocolo IROBEX (3Com Palm Pilot). En la distribución de nombres de dispositivos de `irdadump` se muestra entre paréntesis los protocolos soportados por el dispositivo. El soporte del protocolo IrLAN está en proceso "work in progress": en este momento aún no es estable, pero estará disponible con Linux próximamente.

Solución de problemas

Si los dispositivos en el puerto de infrarrojos no reaccionan, se puede comprobar con el comando `irdadump` si el ordenador llega a reconocer el otro dispositivo:

`irdadump`

Si hay una impresora Canon BJC-80 "a la vista" del ordenador, aparece el siguiente mensaje en la pantalla, repitiéndose periódicamente (ver salida en pantalla 13).

```
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=* erde
                    hint=0500 [ PnP Computer ] (21)
```

Mensaje en pantalla 13: IrDA: irdadump

Si no aparece nada en pantalla o el otro dispositivo no responde, debe comprobar primero la configuración de la interfaz. ¿Realmente está usando la interfaz correcta? Esta se encuentra a veces también en `/dev/ttyS2` o `/dev/ttyS3` y también puede que se use otra interrupción que no sea la 3. En casi todos los portátiles es posible modificar esta configuración en la BIOS.

Con una sencilla cámara de vídeo puede comprobar si el diodo LED se ilumina realmente; en contraposición a los ojos humanos, la mayoría de las cámaras de vídeo pueden ver la luz infrarroja.

Parte III

El sistema

SuSE Linux en sistemas AMD64

AMD presentó a la opinión pública su procesador AMD Athlon 64 en septiembre de 2003. Este nuevo procesador es de 64 bits y puede por tanto ejecutar los nuevos programas AMD64 de 64 bits al mismo tiempo que permite la ejecución de programas x86 de 32 bits ya existentes con igual rendimiento.

Los programas de 64 bits admiten espacios de direcciones más grandes y ofrecen un mejor rendimiento gracias a registros adicionales (soportados exclusivamente en modo de 64 bits) y a otras novedades como las modernas convenciones de llamada (ingl. *Calling conventions*) para funciones.

Con este producto, SuSE Linux soporta el nuevo procesador por partida doble:

- SuSE Linux de 32 bits para x86 lo soporta como procesador de 32 bits al igual que soporta los procesadores Athlon de AMD y Pentium de Intel.
- El nuevo SuSE Linux de 64 bits para AMD64 lo soporta en modo de 64 bits. Asimismo se soporta la ejecución y el desarrollo de programas x86 de 32 bits.

Atención

Por razones históricas, la salida del comando `uname -m` es `x86_64`, ya que éste era el nombre de la primera especificación de AMD.

Atención

SuSE Linux de 64 bits para AMD64

Hardware

En la parte del hardware, AMD64 no se diferencia de los sistemas Athlon normales desde el punto de vista del usuario. Las interfaces y buses de uso corriente son idénticos en ambas plataformas y continúan soportándose.

Debido a que los controladores de hardware para Linux en AMD64 han de ser de 64 bits, puede que tengan que ser adaptados parcialmente. Algunas tarjetas antiguas no funcionan en la actualidad, pero el soporte de hardware actual debería ser el mismo en sistemas de 32 y de 64 bits.

Software

En la parte del software, casi todos los paquetes son de 64 bits si bien también se soporta la ejecución de programas de 32 bits. Con este fin se han desarrollado especialmente paquetes de librerías de 32 bits incluidas en la instalación estándar. Para posibilitar la instalación de librerías de 32 y 64 bits homónimas en el mismo sistema, las librerías de 32 bits se instalan en directorios `/lib` mientras que las de 64 bits lo hacen en `/lib64`. De esta forma se consigue que los paquetes RPM de 32 bits puedan ser instalados sin cambios.

Entre los paquetes que no son de 64 bits cabe mencionar OpenOffice y algunos paquetes comerciales como Acrobat Reader.

Desde el punto de vista del administrador y el usuario, la distinción entre 32 y 64 bits no se aprecia directamente, ya que todos los programas presentan el mismo aspecto y comportamiento.

Instalación de software de 32 bits

Puede que sea necesario convencer al software de 32 bits que invoca `uname` para determinar la arquitectura de que funcione en sistemas AMD64. Con este fin puede utilizarse el programa `linux32`. Una vez empleado, la salida de `uname -m` se modifica:

```
$ uname -m
x86_64
$ linux32 uname -m
i686
```

Desarrollo de software en sistemas de 64 bits

Con SuSE Linux para sistemas AMD64 pueden desarrollarse programas 32 y de 64 bits. Los compiladores GNU generan normalmente código AMD64 de 64 bits. El conmutador `-m32` se encarga de crear código x86 de 32 bits que funcione también en sistemas AMD Athlon de 32 bits o Intel Pentium.

Para desarrollar código de 64 bits es necesario utilizar librerías de 64 bits. Aunque las rutas `/lib64` y `/usr/lib64` se examinan siempre, para código

X11 es necesario por ejemplo emplear `-L/usr/X11R6/lib64`. Por lo tanto, puede que haga falta adaptar los makefiles.

Una opción para depurar el código es GDB, el cual se llama `gdb` para programas AMD64 de 64 bits y `gdb32` para programas x86 de 32 bits. La herramienta `strace` es capaz de examinar ambas clases de programas y la librería Tracer `ltrace` dispone también de un programa específico para 32 bits: `ltrace32`.

Información adicional

Puede obtener información adicional en la página web de AMD (www.amd.com) y en la página del proyecto Linux en AMD64 (www.x86-64.org).

El kernel de Linux

El kernel es el corazón del sistema. En las siguientes páginas no aprenderá cómo convertirse en un “hacker” del kernel, pero se explicará cómo se realiza una actualización del kernel, y llegará a ser capaz de compilar e instalar un kernel configurado. Si procede como se indica en este capítulo, el kernel funcionará adecuadamente y lo podrá arrancar en cualquier momento.

Actualización del kernel	256
Las fuentes del kernel	257
Configuración del kernel	257
Módulos del kernel	259
Ajustes en la configuración del kernel	262
Compilación del kernel	262
Instalación del kernel	263
Limpieza del disco después de la compilación	264

El kernel, que se copia al directorio `/boot` durante la instalación, está configurado de tal forma que cubre un amplio espectro de hardware. Por eso en la mayoría de los casos *no es necesario* generar un kernel propio, a no ser que quiera probar utilidades o controladores en fase de experimentación.

Ya existen `makefiles` para la creación de un nuevo kernel; con ayuda de estas el proceso se realiza casi de forma automática. Sólo la selección del hardware y prestaciones que el kernel debe soportar tiene que realizarse de forma interactiva. Puesto que para realizar la selección correcta, debe conocer su sistema bastante bien, le recomendamos – al menos en el primer intento – que modifique archivos de configuración ya existentes y en funcionamiento, con el fin de disminuir el riesgo de una realizar una configuración inadecuada.

Actualización del kernel

Para instalar un kernel de actualización de SuSE, descargue en su ordenador el paquete de actualización del servidor FTP de SuSE o de un mirror como por ejemplo: <ftp://ftp.gwdg.de/pub/linux/suse/>. Si no sabe qué versión del kernel está presente en su sistema, puede examinar la secuencia de versión con:

```
cat /proc/version
```

O bien averiguar a qué paquete pertenece el kernel `/boot/vmlinuz`:

```
rpm -qf /boot/vmlinuz
```

Antes de la instalación haga una copia de seguridad del kernel original y del `initrd` correspondiente. Para ello ejecute los siguientes comandos como `root`:

```
cp /boot/vmlinuz /boot/vmlinuz.old  
cp /boot/initrd /boot/initrd.old
```

Instale ahora el nuevo paquete con el comando:

```
rpm -Uvh <nombre_paquete>
```

Introduzca el número de versión correspondiente.

A partir de SuSE Linux 7.3 se utiliza `reiserfs` como sistema de archivos estándar, lo que presupone un "initial ramdisk". Este se escribirá de nuevo con el comando `mk_initrd`. En el caso de versiones actuales de SuSE Linux, esto sucede automáticamente durante la instalación del kernel.

Si se da el caso de que quiere arrancar el antiguo kernel, debe configurar el cargador de arranque (ingl. *bootloader*) de forma correspondiente. Para obtener más información consulte el capítulo [El proceso de arranque y el gestor de arranque](#) en la página 73.

Si desea instalar el kernel original de los CDs de SuSE Linux, el proceso es similar. En el directorio `suse/images` del CD1 o DVD puede encontrar el kernel estándar como paquete rpm. Instálelo como se ha descrito anteriormente. En caso de que reciba un mensaje de error indicando que ya existe un nuevo paquete instalado, añada la opción `--force` al comando rpm.

Las fuentes del kernel

Para poder generar un kernel propio se deben instalar las fuentes del kernel (paquete `kernel-source`). El resto de los paquetes necesarios – el compilador de C (paquete `gcc`), los GNU Binutils (paquete `binutils`) y las librerías de C (Include-files) (paquete `glibc-devel`) – se instalarán automáticamente.

Tras la instalación, las fuentes del kernel se encuentran en el directorio `/usr/src/linux-<kernel-versión>`. SuSE. Si le gusta experimentar con el kernel y tener varias versiones en el disco, resulta bastante práctico desempaquetar las fuentes de los diferentes kernel en diferentes directorios y acceder a las actualmente válidas mediante un enlace, ya que existen paquetes de software que esperan encontrar las fuentes del kernel de `/usr/src/linux`. YaST instala los paquetes de esta forma automáticamente.

Configuración del kernel

La configuración del kernel que se instaló en el sistema durante la instalación o actualización está contenida en el archivo `/boot/vmlinuz.config`. Para modificar esta configuración conforme a sus necesidades, cambie como usuario `root` al directorio `/usr/src/linux` y ejecute bien el comando `make oldconfig` que creará el archivo `.config`, o bien el siguiente comando:

```
cp /boot/vmlinuz.config /usr/src/linux/.config
```

De manera alternativa, puede utilizar la configuración del kernel ejecutándose en ese momento. Esto se realiza en SuSE Linux del siguiente modo:

```
zcat /proc/config.gz > /usr/src/linux/.config
```

Las herramientas de configuración del kernel evalúan entonces el archivo `.config`. El kernel se puede configurar de tres formas distintas: mediante la

línea de comandos, mediante un menú en modo texto, o mediante un menú en sistema X Window. A continuación se presentan brevemente estos tres modos.

Configuración en la línea de comandos

Para configurar el kernel, cambie a `/usr/src/linux` e introduzca el siguiente comando:

```
make config
```

A continuación aparece una serie de preguntas sobre las funciones que el kernel debe soportar y para contestarlas existen generalmente dos o tres posibilidades: Ya sea el sencillo **(y)** o **(n)** o bien **(y)** (ingl. *yes*), **(n)** (ingl. *no*) o **(m)** (ingl. *module*). 'm' significa que el controlador correspondiente no se incorpora fijo en el kernel, sino que es posible "añadirlo" en tiempo de ejecución.

Por supuesto, todos los controladores que se necesitan para arrancar el sistema deben incorporarse de forma fija al kernel; para estos módulos pulse **(y)**. Pulse **(Intro)** para confirmar la selección que se leerá de `.config`. Al presionar cualquier otra tecla, aparece una ayuda corta sobre la correspondiente opción.

Configuración en modo texto

Una vía más asequible para configurar el kernel se consigue con "menuconfig", para lo que debe instalar el paquete(ncurses-devel) con YaST. Arranque la configuración del kernel con el comando `make menuconfig`.

Si el cambio en la configuración es pequeño, no tiene por qué pasar por todas las preguntas. sino que también puede elegir directamente en el menú los campos que le interesan. Las configuraciones predeterminadas se encuentran en `.config`. Para cargar otra configuración, escoja el punto del menú 'Load an Alternate Configuration File' e introduzca el nombre del archivo.

Configuración mediante sistema X Window

Si están instalados los paquetes sistema X Window (paquete `xf86`), Tcl/Tk (paquete `tcl` y paquete `tk`), queda la alternativa de iniciar el proceso de instalación con:

```
make xconfig
```

De este modo se dispone de una interfaz gráfica más confortable pero es preciso iniciar el sistema X Window como superusuario `root` o bien introducir primero en Shell `xhost +` como usuario normal para poder tener acceso a la pantalla

como `root`. Las configuraciones predeterminadas se encuentran en `.config`, por lo que mientras no realice una nueva configuración, las configuraciones en este archivo son las que se corresponden con el kernel estándar de SuSE. Tenga presente que el mantenimiento en la configuración mediante `make xconfig` no es tan bueno como con las otras opciones de configuración. Por este motivo, siempre debería ejecutar un `make oldconfig` después de esta configuración. No olvide tampoco volver a generar las dependencias después de un cambio en la configuración. Independientemente del método de configuración utilizado, ha de ejecutar al final el siguiente comando:

```
make dep
```

Esto es necesario sobre todo si desea construir módulos del kernel para software comercial.

Módulos del kernel

Existe una gran cantidad de componentes de hardware para PCs. Para utilizar este hardware correctamente, se necesita un controlador que haga de intermediario entre el sistema operativo (en Linux es el kernel) y el hardware. Normalmente existen dos mecanismos para integrar controladores en el kernel:

- Controladores unidos al kernel. En este manual denominaremos a este tipo de kernel "de una sola pieza" como *kernel monolítico*. Algunos controladores sólo pueden funcionar de esta forma.
- Controladores cargados en el kernel cuando se necesitan, lo que denominaremos como *kernel modularizado*. La ventaja aquí es que sólo se cargan los controladores que se necesitan realmente y por lo tanto el kernel no contiene ninguna carga innecesaria.

En la configuración del kernel se define qué controladores se unirán al módulo y cuáles se añadirán como módulos. Todos los componentes del kernel que no sean necesarios durante el proceso de arranque deberán añadirse como módulos. De esta forma nos aseguramos de que el kernel no aumente excesivamente de tamaño, lo que provocaría dificultades al ser cargado por la BIOS y por el cargador de arranque (ingl. *bootloader*). El controlador de los discos duros, soporte para `ext2` y otros similares se suelen compilar directamente en el kernel; mientras que el soporte para `iso9660`, `msdos` o `sound` se debe compilar como módulo.

Los módulos del kernel se guardan en el directorio `/lib/modules/<pathversión>`, donde `<versión>` corresponde a la versión actual del kernel.

Detectar el hardware actual con hwinfo

SuSE Linux incluye el programa `hwinfo` con el que puede detectar el hardware actual de su ordenador para asignar así los controladores disponibles. Puede obtener unas líneas de ayuda sobre este programa con el comando

```
hwinfo --help
```

Por ejemplo, para obtener los datos del dispositivo SCSI integrado, utilice el siguiente comando:

```
hwinfo --scsi
```

El resultado de este programa de ayuda se encuentra también en el módulo de información de hardware de YaST.

Manejo de los módulos

Existen los siguientes comandos para trabajar con módulos:

- **insmod**
El comando `insmod` carga el módulo indicado que se busca en un subdirectorio de `/lib/modules/<Version>`. Se recomienda dejar de usar `insmod` en favor del comando `modprobe` (ver abajo).
- **rmmod**
Este comando descarga el módulo indicado, lo cual solo es posible cuando se ha dejado de usar esta función del módulo, y no es posible descargar p. ej. el módulo `isofs` cuando todavía hay un CD montado.
- **depmod**
Este comando genera en el directorio `/lib/modules/<versión>` el archivo `modules.dep` que registra la dependencia de los módulos entre sí. De este modo hay seguridad de que se cargan automáticamente todos los módulos que dependen del primero. El archivo con las dependencias de los módulos se genera automáticamente cuando Linux se inicia (salvo que el archivo ya exista).
- **modprobe**
Carga o descarga de un módulo considerando las dependencias con otros. El comando es muy versátil así que se puede usar para muchas otras cosas (p. ej. para probar todos los módulos de un determinado tipo hasta que se cargue uno exitosamente). Al contrario de `insmod`, `modprobe` evalúa el archivo `/etc/modules.conf` y por eso solo se debería usar para cargar

módulos. La página de manual de `modprobe` explica todas las posibilidades.

- **lsmod**

Muestra los módulos actualmente cargados y sus dependencias. Los módulos que fueron cargados por el `kernel-daemon` se identifican por (`autoclean`) al final de la línea. Esta palabra indica que se trata de un módulo que se descarga automáticamente cuando deja de ser usado para un determinado tiempo y si se hayan tomado las medidas necesarias para ello, ver en esta página.

- **modinfo**

Muestra información sobre un módulo.

/etc/modules.conf

El archivo `/etc/modules.conf` influye sobre la carga de módulos (ver página del manual de `depmod` (`man depmod`)).

Este archivo permite indicar los parámetros para aquellos módulos que acceden directamente al hardware y por lo tanto deben ser adaptados específicamente al ordenador (p.ej. controlador de unidades CD-ROM o controlador para tarjetas red). Los parámetros aquí mencionados se describen en las fuentes del kernel. Instale con este fin el paquete `kernel-source` y lea la documentación en el directorio `/usr/src/linux/Documentation`.

Kmod – el cargador de módulos del kernel (ingl. *Kernel Module Loader*)

El modo más elegante para emplear módulos de kernel es el uso del cargador de módulos del kernel. `Kmod` permanece en segundo plano y se ocupa de cargar automáticamente los módulos con llamadas a `modprobe` cuando se necesita la correspondiente función del kernel.

Para usar el `Kmod` se debe activar, durante la configuración del kernel, la opción 'Kernel module loader' (`CONFIG_KMOD`).

`Kmod` no está diseñado para descargar automáticamente módulos; pensando en la cantidad de memoria RAM de los ordenadores de hoy en día, se trata de un operación no necesaria, ya que con la descarga de un módulo se desocuparía muy poca memoria (ver `/usr/src/linux/Documentation/kmod.txt`). Los servidores que cumplen tareas muy específicas trabajan más rápido con un kernel "monolítico".

Ajustes en la configuración del kernel

Debido a la gran cantidad no es posible detallar en este manual todas las opciones que ofrece la configuración del kernel, pero se puede usar la amplia ayuda en línea de la que se dispone durante la configuración del kernel. Lo más nuevo en cuanto a documentación se encuentra siempre en el paquete de las fuentes del kernel en el directorio `/usr/src/linux/Documentation` (siempre y cuando el paquete `kernel-source` esté instalado).

Compilación del kernel

Recomendamos generar un "bzImage" con el cual se evita el efecto de un kernel demasiado grande. Es algo que ocurre a menudo cuando se han seleccionado demasiadas características y luego se genera un "zImage". Con "bzImage" se evitan entonces los mensajes típicos como "kernel too big" o "System is too big".

Una vez adaptado el kernel a sus necesidades, debe iniciar la compilación con (en `/usr/src/linux/`:

```
make dep
make clean
make bzImage
```

Pueden introducir también los tres comandos en una sola línea:

```
make dep clean bzImage
```

Después de una compilación correcta, pueda encontrar el kernel comprimido en `/usr/src/linux/arch/i386/boot`La imagen del kernel – el archivo que contiene el kernel – se llama `bzImage`.

Si este no se encuentra en el mencionado directorio, lo más probable es que haya ocurrido un error durante la compilación.

Si se trabaja con el `bash`, se puede volver a iniciar el proceso de compilación y dejar que se escriba en el archivo `kernel.out`:

```
make bzImage 2>&1 | tee kernel.out
```

Si hay funciones del kernel que se realizan con módulos, es preciso compilarlos, lo cual se consigue con el siguiente comando:

```
make modules
```

Instalación del kernel

Después de la compilación del kernel se debe procurar también que éste se inicie; si se usa LILO para arrancar, es preciso reinstalarlo. Lo más fácil es copiar el nuevo kernel a `/boot/vmlinuz` e iniciar después LILO.

Sin embargo, es mejor conservar el kernel antiguo (como `/boot/vmlinuz.old`) para evitar sorpresas en caso de que el nuevo no funcione como se espera:

```
cp /boot/vmlinuz /boot/vmlinuz.old
cp arch/i386/boot/bzImage /boot/vmlinuz
lilo
```

El comando `make bzlilo` realiza estos tres pasos con una sola orden.

Atención

En caso de utilizar GRUB como cargador de arranque, *no* es necesario reinstalar éste. Así pues, realice sólo los dos primeros pasos para copiar el kernel en el lugar adecuado del sistema.

Atención

Los módulos compilados también se deben instalar. El siguiente comando:

```
make modules_install
```

los copia en los directorios de destino correctos (`/lib/modules/<versión>`). Los módulos antiguos de la misma versión de kernel se suprimen. Esto no representa mucho problema ya que se pueden instalar nuevamente desde los CDs, junto con el kernel.

Truco

Si se incorporan módulos al kernel, es necesario quitarlos en `/lib/modules/<versión>`, ya que en caso contrario pueden aparecer efectos extraños. Por eso se ruega encarecidamente a los principiantes en materia de Linux, no compilar un kernel propio.

Truco

Para que LILO o GRUB puedan arrancar el kernel antiguo (ahora `/boot/vmlinuz.old`), introduzca en el archivo `/etc/lilo.conf` o `/boot/grub/menu.lst` una etiqueta adicional `linux.old` como imagen de arranque (ingl. *boot-image*). Este procedimiento se describe de forma detallada en el capítulo [El proceso de arranque y el gestor de arranque](#) en la página 73.

Si utiliza LILO como cargador de arranque, ha de volver a ejecutar `lilo` cada vez que modifique el archivo `/etc/lilo.conf`. En el caso de GRUB no es necesario reinstalarlo.

Además tenga en cuenta lo siguiente: el archivo `/boot/System.map` contiene los símbolos del kernel necesarios para que los módulos puedan acceder correctamente a las funciones del kernel. Este archivo depende de la versión actual del kernel por lo que se debería copiar el archivo actual (después de cada compilación este archivo se genera de nuevo) `/usr/src/linux/System.map` al directorio `/boot` una vez que la compilación haya finalizado. Si se usa el comando `make bzlilo` o `make zlilo` para generar el kernel, la mencionada copia se hace automáticamente.

Un mensaje como "System.map does not match actual kernel" durante el arranque del sistema, indica que el archivo `System.map` no se ha copiado al directorio `/boot`.

Limpieza del disco después de la compilación

Los archivos objeto que se generan durante la compilación del kernel se pueden borrar si ocupan demasiado espacio de disco:

```
cd /usr/src/linux
make clean
```

Sin embargo, si dispone de suficiente espacio de disco y además piensa modificar la configuración del kernel puede saltarse este paso. De este modo la nueva compilación se lleva a cabo mucho más rápido, ya que sólo se compilan las partes del sistema que han sido modificadas.

Características del sistema

Indicaciones sobre *Filesystem Hierarchy Standard* (FHS) y *Linux Standard Base* (LSB), paquetes individuales de software y particularidades, como el "initrd" al arrancar, el programa `linuxrc` y el "sistema de rescate".

Estándares de Linux	266
Entornos de ejemplo para FTP y HTTP	266
Observaciones sobre paquetes especiales	267
Arrancar con initial ramdisk	273
<code>linuxrc</code>	278
El sistema de rescate de SuSE	283
Consolas virtuales	289
Distribución del teclado	289
Configuración nacional – I18N/L10N	291

Estándares de Linux

Filesystem Hierarchy Standard (FHS)

SuSE Linux intenta cumplir al máximo el estándar sobre jerarquía del sistema de ficheros (ingl. *Filesystem Hierarchy Standard*) (FHS, paquete `fhs`), véase <http://www.pathname.com/fhs/>. Por lo tanto a veces es necesario mover ficheros o directorios al lugar "correcto" en el árbol de directorios, tal y como está establecido en FHS.

Linux Standard Base (LSB)

SuSE soporta activamente los esfuerzos del proyecto *Linux Standard Base*, sobre el cual es posible informarse en <http://www.linuxbase.org>.

La especificación de LSB existe en la versión 1.3.x; el estándar sobre jerarquía del sistema de ficheros (FHS) forma ahora parte del LSB, y entre otras cosas incluye una especificación del formato de paquetes y de la inicialización del sistema; véase el capítulo 12 en la página 295

teTeX – TeX en SuSE Linux

T_EX es un completo sistema que funciona en una gran cantidad de plataformas y se puede ampliar mediante paquetes macros como L^AT_EX. Está compuesto de muchos ficheros individuales, que se combinan conforme a la *estructura de directorios* T_EX (TDS, T_EX Directory Structure) (véase <ftp://ftp.dante.de/tex-archive/tds/>). teTeX es la combinación del actual software T_EX.

Con SuSE Linux, teTeX está disponible con una configuración que cumple las exigencias tanto de TDS como de FHS.

Entornos de ejemplo para FTP y HTTP

Sobre FTP

El paquete `ftpd` contiene un entorno de ejemplo para facilitar la configuración de un servidor FTP. Este entorno se instala en `/srv/ftp`.

Sobre HTTP

El servidor web predeterminado de SuSE Linux es Apache, que se instala junto con algunos documentos de ejemplo en el directorio `/srv/www`. Para poner en marcha un servidor de web propio se recomienda definir un `DocumentRoot` propio en el fichero `/etc/httpd/httpd.conf` en el que colocará sus ficheros (documentos, imágenes, etc.).

Observaciones sobre paquetes especiales

El paquete bash y `/etc/profile`

Cuando se le llama como shell de login, bash utiliza los ficheros de inicialización en el siguiente orden:

1. `/etc/profile`
2. `~/.profile`
3. `/etc/bash.bashrc`
4. `~/.bashrc`

Los usuarios pueden efectuar las entradas propias en `~/.profile` o `~/.bashrc`. Para garantizar el trabajo ordenado de estos ficheros, recomendamos hacerse cargo de la configuración básica actual de `/etc/skel/.profile` o `/etc/skel/.bashrc` en el directorio del usuario. Por tanto, después de una actualización le recomendamos que recoja las configuraciones de `/etc/skel`; para no perder las propias adaptaciones, ejecute los siguiente comandos en la shell:

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

Una vez hecho, puede buscar sus adaptaciones en los ficheros `*.old`.

El paquete cron

Las tablas de cron se encuentran en `/var/spool/cron/tabs`. El fichero `/etc/crontab` se genera como tabla de comandos para todo el sistema. En este fichero hay que anotar, además de la hora, el usuario que ha encargado la tarea a ejecutar (ver fichero 22, en el que figura `root` como usuario); las tablas específicas de los paquetes (en `/etc/cron.d`) siguen la misma filosofía – ver página del manual de cron (`man 8 cron`).

```
1-59/5 * * * * root test -x /usr/sbin/atrun && /usr/sbin/atrun
```

Fichero 22: Ejemplo de entrada en /etc/crontab

No se puede usar el comando `crontab -e` para modificar `/etc/crontab`; se debe modificar con un editor y posteriormente grabarlo.

Hay algunos paquetes que instalan scripts dentro de los directorios `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` y `/etc/cron.monthly`. De la ejecución de estos se encarga `/usr/lib/cron/run-crons`, que se inicia cada 15 minutos desde la tabla principal (`/etc/crontab`).

Las tareas diarias de mantenimiento del sistema están divididas en varios scripts en aras de la claridad. (paquete `aaa_base`). Por tanto, en `/etc/cron.daily` puede encontrar junto a `aaa_base` p.ej. los componentes `backup-rpmdb`, `clean-tmp` o `clean-vi`.

Archivos de registro – el paquete logrotate

Muchos servicios del sistema ("Daemons") y también el kernel mismo vuelcan periódicamente el estado del sistema y sucesos especiales en archivos de registro (ingl. *logfiles*). Así el administrador puede controlar de forma eficaz en que estado se encontró el sistema en un momento determinado, detectar errores o funciones erróneas y solucionarlos adecuadamente. Estos archivos de registro se guardan según el FHS en `/var/log` y aumentan cada día su tamaño. Con ayuda del paquete `logrotate` se puede controlar el crecimiento de los archivos de registro.

Migración a logrotate (8.0)

Al actualizar una versión anterior a SuSE Linux 8.0 se guardan parámetros de la configuración anterior:

- Se mueven a `/etc/logrotate.d/aaa_base` las entradas de `/etc/logfile`, que no están relacionadas con un paquete concreto.
- La antigua variable de `rc.config` `MAX_DAYS_FOR_LOG_FILES` se representa como `dateext` y `maxage` en el fichero de configuración; ver página del manual de `logrotate` (`man 8 logrotate`).

Configuración

El fichero de configuración `/etc/logrotate.conf` define el comportamiento general. Mediante la indicación `include` se determina principalmente qué ficheros se deben evaluar; en SuSE Linux está previsto que los paquetes individuales instalen ficheros en `/etc/logrotate.d` (p.ej. `syslog` o `yast`).

```
# 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.
```

Fichero 23: Ejemplo de `/etc/logrotate.conf`

`logrotate` se controla con `cron`; se arranca una vez al día mediante `/etc/cron.daily/logrotate`.

Atención

La opción `create` no reconsidera eventuales ajustes efectuados como administrador en los ficheros `/etc/permissions*`. Por favor, asegúrese de que no se produzcan conflictos al realizar sus propios ajustes.

Atención

Páginas man

Para algunos programas GNU, no se siguen manteniendo las páginas man (p. ej. `tar`). En su lugar se puede usar como ayuda rápida la extensión `--help` o los ficheros del tipo `info`. `Info (info)` es el sistema de hipertexto de GNU cuyo uso se explica con el comando `info info`. Se puede llamar a `info` a través de Emacs con el comando `emacs -f info` o también sólo con el comando `info`. De uso agradable son `tkinfo`, `xinfo` o el acceso a través del sistema de ayuda.

El comando ulimit

El comando `ulimit` (ingl. *user limits*) permite limitar los recursos del sistema o visualizarlos. `ulimit` es especialmente útil para limitar el uso de la Memoria por parte de las aplicaciones. Así es posible evitar que una aplicación se reserve demasiada o toda la memoria, lo que podría provocar el cuelgue del sistema.

`ulimit` tiene varias opciones; las que limitan el gasto de memoria figuran en la tabla 11.1.

- m Tamaño máximo de memoria RAM
- v Tamaño máximo del fichero de intercambio (Swap)
- s Tamaño máximo de las pilas
- c Tamaño máximo de los fichero core
- a Mostrar límites establecidos

Cuadro 11.1: `ulimit`: Limitar los recursos para el usuario

Los límites para todo el sistema se pueden establecer en `/etc/profile`. También es en este fichero donde se debe dar de alta la creación de los ficheros core, que necesitan los programadores para depurar código (ingl. *debugging*). Los usuarios no pueden aumentar los valores que el administrador del sistema define

en `/etc/profile`, pero sí que pueden hacer una configuración personal en `~/.bashrc`.

```
# Limitar la memoria RAM:
ulimit -m 98304

# Limitar la memoria virtual (swap):
ulimit -v 98304
```

Fichero 24: Establecer límites con `ulimit` en `/etc/bashrc`

Todos los valores se han de indicar en KB. Información más detallada se encuentra en página del manual de `bash` (`man bash`).

Atención

No todas las shells soportan entradas para `ulimit`. Si debe realizar una configuración más avanzada, PAM (p.ej. `pam_limits`) le ofrece más posibilidades.

Atención

El comando `free`

El comando `free` es bastante engañoso cuando se trata de averiguar la memoria de trabajo que se está utilizando...

Puede encontrar información útil en `/proc/meminfo`. Hoy en día no se debería preocupar por esto ningún usuario que utilice un sistema de trabajo moderno como Linux. El concepto de "memoria de trabajo libre" viene de la época en que aún no existía ningún administrador de memoria unificado (ingl. *unified memory management*). En Linux existe el lema: *memoria libre es memoria mala* (ingl. *free memory is bad memory*). Como consecuencia, Linux siempre se esfuerza por equilibrar el uso de la memoria caché sin llegar nunca a dejar memoria libre (=sin usar).

Básicamente, el kernel no sabe directamente de programas o datos de usuarios; se dedica a administrar programas y datos en los denominados "page cache".

Cuando la memoria se queda pequeña, algunos trozos se escriben en la zona de intercambio (ingl. *swap*) o en los ficheros de los cuales leía al principio con ayuda de `mmap`; véase página del manual de `mmap` (`man 2 mmap`).

Además el kernel dispone de otra memoria caché adicional, como la "slab cache", que p.ej. contiene los búferes empleados para el acceso a redes. De

esta forma se solucionan las diferencias que puedan surgir entre los contadores de `/proc/meminfo`. La mayoría, pero no todos, se pueden pedir en `/proc/slabinfo`.

El fichero `/etc/resolv.conf`

La resolución de nombres se regula en el fichero `/etc/resolv.conf`; véase apartado *DNS – Domain Name System* en la página 339.

Sólo el script `/sbin/modify_resolvconf` se encarga de modificar el fichero `/etc/resolv.conf`. Ningún programa por sí mismo tiene el derecho de actualizar `/etc/resolv.conf`. La configuración de red y los datos correspondientes sólo se pueden mantener consistentes si se cumple siempre esta regla.

Configuración de GNU Emacs

GNU Emacs es un entorno de trabajo bastante complejo. Puede encontrar más información sobre el mismo en:

ver <http://www.gnu.org/software/emacs/>.

En los siguientes párrafos se mencionan los ficheros de configuración que GNU Emacs procesa durante el inicio.

Al iniciarse, Emacs lee diversos ficheros para adaptarse o preconfigurarse conforme a las especificaciones del usuario, administrador de sistemas o del distribuidor según corresponda.

El fichero de inicio `~/.emacs` es instalado en el directorio local de cada usuario por `/etc/skel`; `.emacs` lee a su vez el fichero `/etc/skel/.gnu-emacs`. Si un usuario desea modificar este fichero, se recomienda copiarlo en el propio directorio local de usuario y allí realizar los cambios deseados:

```
cp /etc/skel/.gnu-emacs ~/.gnu-emacs
```

El fichero `~/.gnu-emacs-custom` es creado en `.gnu-emacs` como `custom-file`. Si el usuario quiere realizar su propia configuración por medio de `customize`, los cambios se guardarán en `~/.gnu-emacs-custom`.

Junto con paquete `emacs` se instala en SuSE Linux el fichero `site-start.el` en el directorio `/usr/share/emacs/site-lisp`. El fichero `site-start.el` se carga *antes* que el fichero de inicio `~/.emacs`. `site-start.el` se ocupa, por ejemplo, de cargar automáticamente ficheros de configuración que han sido instalados con paquetes complementarios de Emacs incluidos en la distribución

(ej. paquete `psgml`). Tales ficheros de configuración se encuentran también en `/usr/share/emacs/site-lisp` y comienzan siempre con `suse-start-`.

El administrador local de sistemas puede definir opciones de configuración válidas en todo el sistema con `default.el`.

El fichero `info` sobre Emacs en el nodo *Init File*: `info:/emacs/InitFile`, contiene más información sobre estos ficheros. Allí también se describe cómo evitar que se carguen los mismos (en caso de que sea necesario).

Los componentes de Emacs están distribuidos en varios paquetes:

- Paquete básico `emacs`.
- Además hay que instalar normalmente el paquete `emacs-x11`, el cual contiene el programa *con* soporte para X11.
- En el paquete `emacs-nox` se incluye el programa *sin* soporte X11.
- paquete `emacs-info`: documentación en línea en formato `info`.
- paquete `emacs-el` contiene los ficheros de librerías no compiladas en Emacs Lisp. Actualmente no es necesario.
- Numerosos paquetes adicionales que pueden ser instalados en caso necesario: paquete `emacs-auctex` (para $\text{\LaTeX}$); paquete `psgml` (para SGML/XML); paquete `gnuserv` (para el uso de cliente y servidor), etc.

Arrancar con `initial ramdisk`

Situación de arranque

En cuanto el kernel de Linux está cargado y el sistema de archivos raíz (`/`) montado, es posible ejecutar programas y cargar otros módulos de kernel para proporcionar funciones adicionales.

Para llegar al punto de montar el sistema de archivos raíz, se tienen que cumplir varias condiciones.

Por una parte, el kernel necesita el controlador para acceder al dispositivo que contiene el sistema de archivos raíz (sobre todo los controladores para SCSI) y por otra parte el kernel tiene que contener el código necesario para leer el sistema de archivos (`ext2`, `reiserfs`, `romfs`, etc.). Además es posible que el sistema de archivos raíz ya esté codificado, con lo cual se tendría que introducir la contraseña para montarlo.

Hay diferentes soluciones para resolver el problema de los controladores de SCSI. Una posibilidad sería un kernel que contenga todos los controladores existentes, lo que tiene como desventaja el aumento de su tamaño y que pueda haber conflictos entre todos los controladores. Otra solución sería proporcionar diferentes kernels, de los que cada uno contenga uno o un par de controladores SCSI. Esta solución es también complicada ya que requiere una gran cantidad de kernels diferentes, cantidad que además se multiplica por las diferentes optimizaciones para Pentium o SMP.

La solución óptima es la de cargar el controlador SCSI como módulo. Esta solución requiere la posibilidad de ejecutar programas del área (de memoria) de usuario antes de montar el sistema de archivos raíz. Este procedimiento se puede realizar mediante el concepto del *initial ramdisk* (disco de memoria inicial).

El concepto "initial ramdisk"

Los problemas mencionados arriba se resuelven mediante el *initial ramdisk* (también denominado "initdisk" o "initrd"). El kernel de Linux ofrece la posibilidad de cargar un sistema de archivos pequeño a un disco de memoria (ramdisk) para ejecutar programas dentro del mismo antes del montaje real del sistema de archivos raíz. El "bootloader" (GRUB, LILO, etc.) se encarga de cargar el *initrd*. Todos los "bootloader" sólo necesitan rutinas de la BIOS para leer los datos del disco. Cuando el "bootloader" es capaz de cargar el kernel, este también puede cargar el disco de memoria inicial por lo que ya no se necesitan controladores especiales.

Procedimiento del arranque con *initrd*

El "bootloader" carga el kernel y la *initrd* a la memoria e inicia el kernel, indicándole la existencia de un disco de memoria *initrd* y su posición en la memoria.

Normalmente el *initrd* está comprimido, por lo que el kernel lo descomprime y lo monta como sistema de archivos temporal. Después de esto, dentro del disco *initrd* se inicia un programa denominado *linuxrc*, que es capaz de montar el sistema de archivos "normal". En el momento que *linuxrc* finaliza, el disco temporal *initrd* se desmonta y el proceso de arranque sigue en su secuencia habitual, montando el sistema de archivos raíz verdadero. El montaje de *initrd* y la ejecución de *linuxrc* se pueden observar como pasos intermedios durante el proceso de arranque normal.

Después de montar las particiones raíz verdaderas el kernel intenta de remontar el `initrd` al directorio `/initrd`. En caso de error, p. ej. porque el punto de montaje no existe, el kernel intentará desmontar el `initrd`. Si esto fracasa también el sistema es completamente operativo, pero nunca será posible liberar el espacio de memoria que `initrd` ocupa.

El programa `linuxrc`

Las condiciones para `linuxrc` dentro del `initrd` son las siguientes: Debe tener el nombre especial `linuxrc` y se debe encontrar dentro del directorio raíz del `initrd`. Aparte de esto sólo hace falta que el kernel lo pueda ejecutar. Esto significa que `linuxrc` puede ser un programa con enlace (ingl. *link*) dinámico a las librerías, pero en este caso las librerías compartidas (ingl. *shared libraries*) se deben encontrar como es usual bajo `/lib` en el `initrd`. `linuxrc` también podría ser un script de la shell, pero para esto debería existir una Shell en `/bin`. Resumiendo, se puede decir que el `initrd` debe contener un sistema Linux mínimo que permita ejecutar el programa `linuxrc`. Durante la instalación de SuSE Linux se usa un `linuxrc` enlazado estáticamente para mantener el `initrd` lo más pequeño posible, ya que el espacio en los disquetes de arranque es muy reducido. `linuxrc` se ejecuta con derechos de superusuario `root`.

El auténtico sistema de archivos raíz

En cuanto `linuxrc` termina, el `initrd` se desmonta y el proceso de arranque continúa, con el kernel montando el sistema de archivos raíz verdadero. `linuxrc` puede influir sobre el tipo de sistema de archivo raíz que se va a montar. Para ello solo es necesario que `linuxrc` monte el sistema de archivos `/proc` y escriba el valor del sistema de archivos raíz en forma numérica en `/proc/sys/kernel/real-root-dev`.

Cargadores de arranque

La mayoría de los "cargadores/gestores de arranque" (ingl. *bootloader/bootmanager*) funciona con `initrd` (especialmente GRUB, LILO y syslinux). La forma de indicar a los "bootloader" que usen un `initrd` es la siguiente:

GRUB Introducir la siguiente línea en `/boot/grub/menu.lst`:

```
initrd (hd0,0)/initrd
```

Puesto que la dirección de carga de `initrd` se escribe en la imagen del kernel ya cargada, el comando `initrd` ha de ejecutarse a continuación del comando del kernel.

LILO Introducir la siguiente línea en `/etc/lilo.conf`:

```
initrd=/boot/initrd
```

El archivo `/boot/initrd` es el disco de memoria inicial (*initial ramdisk*). Es posible, pero no necesario, que se encuentre comprimido.

syslinux Apuntar la siguiente línea en `syslinux.cfg`:

```
append initrd=initrd <parámetros adicionales>
```

Uso de `initrd` en SuSE

Instalación del sistema

Ya hace tiempos que se usa el `initrd` para la instalación. El usuario puede cargar módulos en `linuxrc` e introducir los datos necesarios para la instalación (sobre todo el medio fuente). Después `linuxrc` inicia YaST, que se encarga de la instalación. Cuando ésta haya terminado, YaST indica a `linuxrc` el lugar donde se encuentra el sistema recientemente instalado. Seguidamente `linuxrc` anota este valor en `/proc`, se termina y el kernel sigue iniciándose con el sistema recién instalado.

Al instalar SuSE Linux se inicia desde un principio prácticamente el mismo sistema que se acaba de instalar – no está mal. Sólo cuando el kernel en ejecución no concuerda con los módulos que se hayan instalado en el sistema, se efectúa un reinicio del mismo. Esto solo hace falta cuando se ha instalado un kernel para máquinas multiprocesador junto con sus módulos, ya que actualmente SuSE Linux a la hora de arrancar, usa un kernel para ordenadores monoprocesador. Para poder usar todos los módulos, hace falta iniciar el kernel SMP del sistema.

Arrancar el sistema instalado

Anteriormente YaST ofrecía más de 40 kernels para la instalación, diferenciándose unos de otros por diferentes drivers para controladoras SCSI. Esto era necesario para el montaje del sistema de archivos raíz después del arranque. Los demás controladores se podían cargar posteriormente como módulos.

Como ahora ofrecemos kernels optimizados, se trata de un concepto inválido, ya que harían falta más de 100 imágenes de kernel diferentes.

Por lo tanto se usa ahora el `initrd` también para el inicio normal del sistema. El funcionamiento es análogo al de la instalación, con la diferencia de que el `linuxrc` es ahora un sencillo script que sólo se ocupa de cargar unos determinados módulos. Por lo general se carga un solo módulo que es el controlador SCSI, necesario para el acceso al sistema de archivos raíz.

Generar un initrd

El `initrd` (ingl. *initial ramdisk*) se genera mediante el script `mk_initrd`. Los módulos que se han de cargar se definen, en el caso de SuSE Linux, con la variable `INITRD_MODULES` en `/etc/sysconfig/kernel`. Después de una instalación esta variable contiene automáticamente los valores correctos, ya que `linuxrc` reconoce los módulos que se han cargado. Estos se cargan exactamente en el orden de aparición en la variable `INITRD_MODULES`, lo cual es importante cuando se cargan varios controladores SCSI, ya que la enumeración de los discos cambia cuando los módulos se cargan en orden diferente. En realidad sería suficiente cargar sólo el controlador SCSI que proporciona acceso al sistema de archivos raíz. La carga posterior automática de controladores SCSI es complicada (sería difícil secuenciarlo, si también hay discos conectados a la segunda controladora), por lo que preferimos cargar todos los controladores SCSI mediante el `initrd`.

Atención

¡La carga de `initrd` por parte del "bootloader" funciona igual que la carga del kernel mismo (LILO anota en su archivo `map` la ubicación de estos datos) y por eso se requiere una nueva instalación del cargador de arranque después de cada cambio en `initrd`. Esto no es necesario en el caso de `grub`.

Atención

Posibles problemas – Kernel compilado a medida

Después de haber compilado un kernel a medida es posible que aparezcan ciertos problemas comunes. Por ejemplo el controlador de SCSI se ha incorporado fijo al kernel, pero el `initrd` se ha quedado sin cambios. A la hora de arrancar pasa lo siguiente: El kernel ya contiene el controlador para SCSI, que reconoce la controladora. El `initrd` en cambio trata de cargar el controlador otra vez como módulo, lo que puede paralizar el sistema (especialmente en caso del `aic7xxx`). En realidad es un fallo del kernel, ya que no debería ser posible cargar de nuevo un controlador ya existente – el problema en sí ya se conoce por el controlador para el puerto serie.

Existen varias soluciones para solventar este problema: Se configura el controlador como módulo (entonces se carga correctamente con el `initrd`) o bien, se quita la entrada del `initrd` de `/etc/grub/menu.lst` o de `/etc/lilo.conf`. Una solución equivalente sería eliminar el controlador de `INITRD_MODULES` y ejecutar `mk_initrd`; este comando reconoce entonces que no se requiere ningún `initrd`.

El futuro

En el futuro es posible que se use `initrd` para tareas más sofisticadas que la sencilla carga de módulos necesarios para el acceso a /.

- Controlador “high end” EIDE
- Sistema de archivos raíz sobre un software RAID (`linuxrc` configura los dispositivos `md`)
- Sistema de archivos raíz sobre LVM
- Sistema de archivos raíz codificado (`linuxrc` pide una contraseña)
- Sistema de archivos raíz sobre un disco SCSI conectado a una tarjeta PCMCIA.

Información adicional

- `/usr/src/linux/Documentation/ramdisk.txt`
- `/usr/src/linux/Documentation/initrd.txt`
- página del manual de `initrd` (`man 4 initrd`).

linuxrc

`linuxrc` es un programa que se comienza a ejecutar durante el inicio del kernel, antes de arrancar realmente. Esta propiedad es muy ventajosa, ya que permite arrancar un kernel pequeño y modularizado, haciendo posible cargar como módulos los pocos drivers que realmente se necesitan, lo cual se puede hacer incluso desde un disquete de módulos.

`linuxrc` ayuda en caso necesario a cargar manualmente los drivers relevantes para el hardware; aunque hoy en día generalmente se puede confiar en la detección automática de hardware que se realiza antes de arrancar `Yast`. `linuxrc` no sólo sirve para la instalación sino también como herramienta de arranque para un sistema Linux instalado, formando así una especie de disquete de rescate. También sirve para resolver algún problema grave en el disco duro o simplemente cuando se ha olvidado la contraseña de `root`, ya que es posible arrancar un sistema de rescate a base de un ramdisk. Hay más información en el apartado [El sistema de rescate de SuSE](#) en la página 283.

Menú principal

Después de haber ajustado el idioma y el teclado se entra al menú principal de linuxrc (ver figura 1.2 en la página 11). Normalmente se usa linuxrc para arrancar Linux; por consiguiente el punto al que se debe llegar en este momento es la opción 'Iniciar la instalación / Sistema'. Depende del hardware de su ordenador y del propósito de la instalación que se pueda entrar directamente a esta opción; puede encontrar más información en el apartado *Instalación en modo texto con YaST* en la página 8

Ajustes

Se puede realizar ajustes en las opciones 'Idioma', 'Pantalla', 'Teclado' y 'Debug (experto)'.

Información del sistema

Con la opción 'Información del sistema' (figura 11.1) no sólo se pueden ver los mensajes del kernel sino también otros datos importantes, como las direcciones de entrada y salida (ingl. *I/O address*) de las tarjetas PCI o el tamaño de la memoria principal.

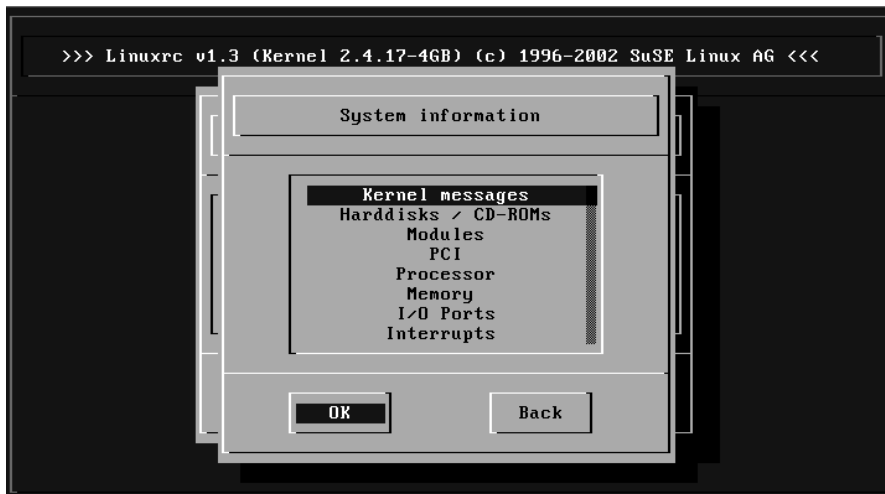


Figura 11.1: Información del sistema

Las siguientes líneas muestran cómo se presenta un disco duro y un lector CD-ROM conectados a una controladora EIDE. Es el caso en el que no hace falta cargar ningún módulo del kernel para la instalación:

```
hda: ST32140A, 2015MB w/128kB Cache, LBA, CHS=1023/64/63
hdb: CD-ROM CDR-S1G, ATAPI CDRom drive
Partition check:
hda: hda1 hda2 hda3 < hda5 >
```

Por otra parte, si se ha arrancado con un kernel que incorpora un driver SCSI, tampoco hace falta cargar ningún módulo SCSI adicional. Las siguientes líneas muestran un mensaje típico de reconocimiento de una controladora SCSI y de los dispositivos conectados:

```
scsi : 1 host.
Started kswapd v 1.4.2.2
scsi0 : target 0 accepting period 100ns offset 8 10.00MHz FAST SCSI-II
scsi0 : setting target 0 to period 100ns offset 8 10.00MHz FAST SCSI-II
Vendor: QUANTUM Model: VP32210 Rev: 81H8
Type: Direct-Access ANSI SCSI revision: 02
Detected scsi disk sda at scsi0, channel 0, id 0, lun 0
scsi0 : target 2 accepting period 236ns offset 8 4.23MHz synchronous SCSI
scsi0 : setting target 2 to period 248ns offset 8 4.03MHz synchronous SCSI
Vendor: TOSHIBA Model: CD-ROM XM-3401TA Rev: 0283
Type: CD-ROM ANSI SCSI revision: 02
scsi : detected 1 SCSI disk total.
SCSI device sda: hwr sector= 512 bytes. Sectors= 4308352 [2103 MB] [2.1 GB]
Partition check:
sda: sda1 sda2 sda3 sda4 < sda5 sda6 sda7 sda8 >
```

Carga de módulos

Aquí se puede elegir qué tipo de módulo se necesita. Si se ha arrancado desde disquete, `linuxrc` carga los datos necesarios y los presenta para elegir.

Si se ha arrancado desde el CD o desde DOS con `loadlin`, todos los módulos ya están a disposición de `linuxrc`. Esto evita la demora en cargar, pero gasta más memoria.

`linuxrc` ofrece los drivers disponibles en una lista. A la izquierda se ve el nombre de cada módulo y a la derecha una breve descripción del hardware para el cual está hecho el módulo (driver).

Para algunos dispositivos existen varios drivers o también unos muy nuevos que aún se encuentran en fase alpha. Estos se ofrecen también aquí.

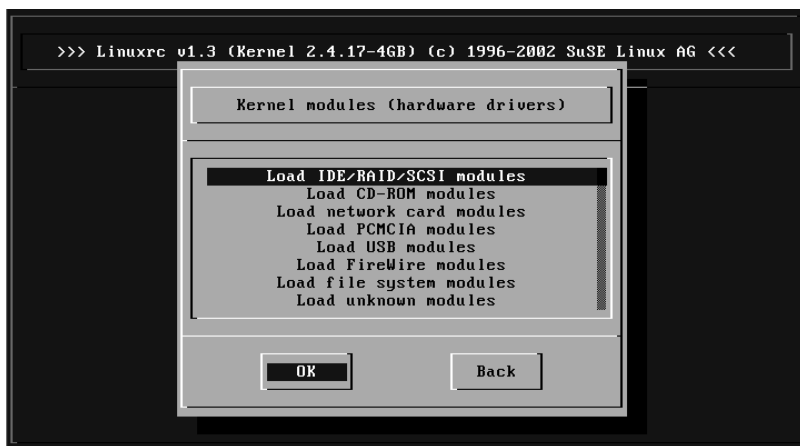


Figura 11.2: Cargar módulos

Introducción de parámetros

Si se ha encontrado el driver que corresponde al hardware, se coloca el cursor sobre la línea en cuestión y se pulsa (↵). Aparece una pantalla con la posibilidad de introducir parámetros que pasarán al módulo que se cargue.

Hay que tener en cuenta aquí, que múltiples parámetros deben estar separados por espacios, contrastando con la introducción de parámetros en el prompt del kernel (MILO, LILO o SYSLINUX).

Por lo general no hace falta especificar el hardware, porque la mayoría de los drivers encuentran los componentes por sí mismos. Solamente las tarjetas de red y lectores CD-ROM con controladora propia exigen a veces la indicación de parámetros. De todos modos se puede probar sencillamente pulsando (↵) sin pasar ningún parámetro.

Algunos módulos necesitan un buen tiempo para reconocer e inicializar el hardware. Cambiando a la consola virtual 4 ((Alt) + (F4)) es posible ver los mensajes del kernel durante la carga del módulo. Sobre todo las controladoras SCSI son las que se toman su tiempo durante la carga, ya que esperan un rato la respuesta de todos los dispositivos conectados.

Cuando se haya cargado el módulo correctamente, linuxrc muestra los mensajes del kernel, así que es posible asegurarse del éxito de la operación. Si no es así, los mensajes pueden servir para encontrar la razón del fracaso.

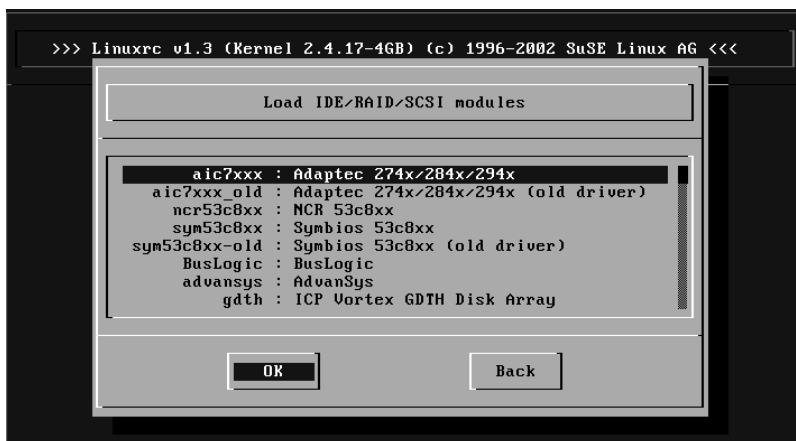


Figura 11.3: Selección de los drivers SCSI

Iniciar la instalación / Sistema

Una vez conseguido el soporte completo del hardware necesario para la instalación, se puede pasar a la opción 'Iniciar la instalación / Sistema'.

En este punto (figura 1.3 en la página 14) se puede comenzar con una serie de procesos: 'Comenzar la instalación' (desde aquí comienza también la actualización), 'Iniciar el sistema instalado' (hace falta conocer la partición raíz), 'Iniciar sistema de rescate' (ver apartado *El sistema de rescate de SuSE* en la página siguiente) 'Sacar CD (eject)'.

La opción 'Iniciar LiveEval-CD' sólo existe después de haber arrancado desde un CD de evaluación (Live-CD). Imágenes de este CD en formato ISO están disponibles en el servidor FTP (`live-eval-<VERSION>`):

<ftp://ftp.suse.com/pub/suse/i386/>

Truco

La opción 'Iniciar LiveEval-CD' es bastante útil a la hora de comprobar la compatibilidad de un determinado ordenador o de un portátil con Linux. Para ello *no* hace falta hacer una instalación real en el disco duro. ¡Se trata de una prueba que se podría efectuar sin más en cualquier tienda de PCs actual!

Truco



Figura 11.4: Introducción de los parámetros para la carga de los módulos

Se pueden elegir diferentes fuentes para la instalación (figura 11.5 en la página siguiente) y también para generar un sistema de rescate (figura 11.6 en la página 286).

El sistema de rescate de SuSE

SuSE Linux contiene varios sistemas de rescate que permiten acceder “desde fuera” a todas las particiones de Linux en los discos duros.

Existe el disquete de arranque y un sistema de rescate que se puede cargar desde un CD, un disquete, la red o desde el servidor FTP de SuSE. Aparte de esto existe un CD arrancable (el “LiveEval-CD”, que puede servir igualmente como sistema de rescate.

El sistema de rescate contiene, entre otras, una buena selección de utilidades para brindar suficientes herramientas que permitan arreglar una serie de problemas, p. ej. imposibilidad de acceso a los discos o problemas con ficheros de configuración. parted(Parted) forma parte del sistema de arranque y sirve para modificar el tamaño de las particiones; en caso de necesidad se le puede invocar manualmente desde el sistema de rescate si no quiere utilizar el modificador de tamaño integrado en /yastii. Puede encontrar más información sobre Parted en:

<http://www.gnu.org/software/parted/>

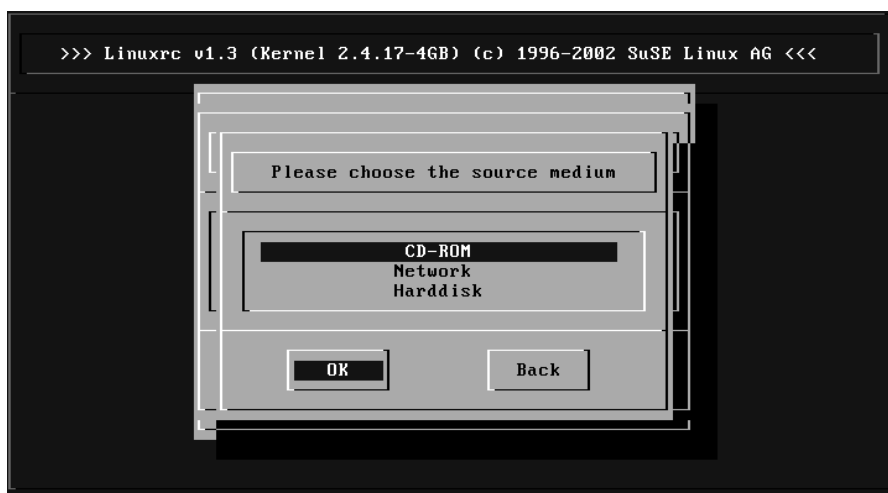


Figura 11.5: Selección del medio fuente en linuxrc

Truco

Siempre se debe mantener los disquetes de arranque y de rescate en un lugar seguro. El pequeño esfuerzo que se necesita para generarlos y mantenerlos no tiene comparación con el trabajo y la pérdida de tiempo que representa no tener nada en un caso de emergencia.

Truco

Preparativos

Para crear el sistema de rescate se necesitan dos disquetes libres de daños: uno como disquete de arranque y el otro para la imagen comprimida de un pequeño sistema de ficheros raíz. El directorio `/disks` en el primer CD contiene las imágenes para el disquete de arranque (`bootdisk`) y para el sistema de rescate `/disks/rescue`.

Hay tres posibilidades para crear el disquete con el sistema de ficheros raíz:

- con YaST
- en una consola de texto con los comandos de Linux:

```
tierra:~ # /sbin/badblocks -v /dev/fd0 1440
```



```
tierra:~ # dd if=/cdrom/disks/rescue of=/dev/fd0 bs=18k
```

o con los equivalentes de DOS (suponiendo aquí que Q: representa el lector CD-ROM bajo DOS):

```
Q:\> cd \dosutils\rawrite Q:\dosutils\rawrite> rawrite.exe
```

El disquete de rescate está actualmente ???(8.1) basado en la librería libc5 (SuSE Linux 5.3); sólo así caben varios programas (un Editor, fdisk, e2fsck, etc.) en un solo disquete.

Atención

No se puede montar el disquete de rescate ya que no contiene ningún sistema de fichero, sino la imagen comprimida de uno. Si se desea verla alguna vez, lea el siguiente párrafo.

Atención

Para contemplar la imagen descomprimida, primero se debe descomprimir y después montarla como usuario `root`. Esto supone que el kernel soporta el *loop-Device* y funciona del siguiente modo:

```
tierra:~ # cp /cdrom/disks/rescue /root/rescue.gz
tierra:~ # gunzip /root/rescue.gz
tierra:~ # mount -t ext2 -o loop /root/rescue /mnt
```

Iniciar el sistema de rescate

El sistema de rescate se inicia desde el disquete de arranque creado anteriormente, desde el CD, o bien desde el DVD de SuSE Linux. Es importante que se pueda arrancar desde la disquetera o desde el lector CD-ROM/DVD respectivamente; si este no fuera el caso se tendría que cambiar el orden de arranque en la BIOS.

A continuación se detallan los pasos para iniciar el sistema de rescate:

1. Arranque el sistema con el disquete de arranque (`bootdisk`) creado anteriormente, el CD, o bien DVD de SuSE Linux.
2. Se puede dejar que el sistema arranque sin intervención o bien se puede seleccionar 'Manual Installation' y – si esto fuera necesario – indicar parámetros en los 'boot options'. Después existe la posibilidad de cargar los módulos de kernel manualmente.

3. Ajuste en `linuxrc` el idioma y el teclado.
4. En el menú principal seleccione 'Iniciar la instalación, sistema'.
5. Si ha arrancado con el disquete de arranque, introduzca el CD de instalación o el disquete (`rescue`) con la imagen comprimida del sistema de rescate.



Figura 11.6: Elección del medio fuente del sistema de rescate

6. En el menú 'Iniciar la instalación / sistema' seleccione la opción 'Iniciar sistema de rescate' (ver figura 1.3 en la página 14) e indique después el medio fuente (ver figura 11.6).

A continuación se explican las diferentes posibilidades a elegir:

'CD-ROM': Al cargar el sistema de rescate, se exporta la ruta `/cdrom`. Lo que hace posible instalar desde *este* CD.

'Red': Para acceder al sistema `rescue` por red hace falta cargar el driver de la tarjeta de red.; ver también los consejos genéricos en el apartado *Instalación desde una fuente en la "red"* en la página 18. En un submenú puede elegir entre varios protocolos: NFS, FTP, SMB etc. (ver figura 11.7 en la página siguiente).

'Disco duro': Cargue el sistema `rescue` desde el disco duro.

'Disquete': Arranque el sistema `rescue` desde un disquete, especialmente si el ordenador tiene poca memoria RAM.

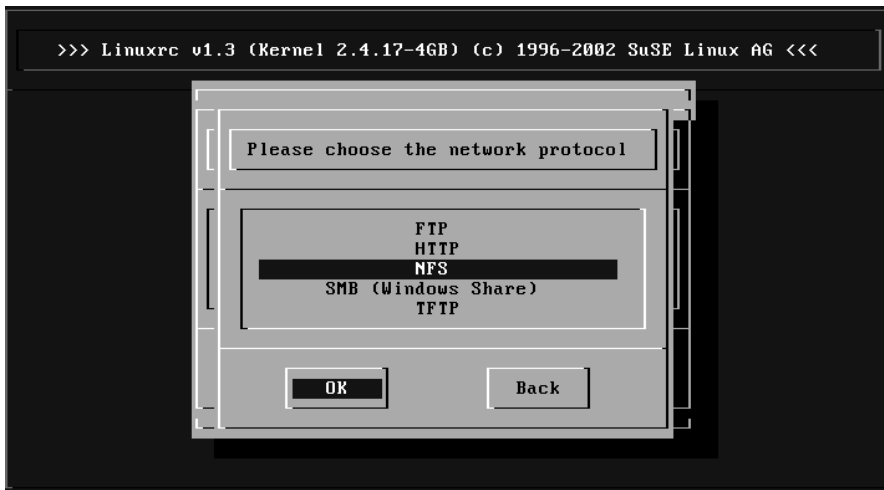


Figura 11.7: Netzwerkprotokolle

Independientemente del medio seleccionado, el sistema de rescate se descomprime y se carga como nuevo sistema de fichero raíz en un "ramdisk" (disco virtual), se monta, arranca y queda así operativo.

Trabajar con el sistema de rescate

El sistema de rescate proporciona, con las teclas **(Alt) + (F1)** hasta **(Alt) + (F3)**, tres diferentes consolas virtuales en las que se puede efectuar un login (entrar en el sistema) como usuario **root** sin necesidad de contraseña. Con las teclas **(Alt) + (F10)** se llega a la consola de sistema para ver los mensajes del kernel y de syslog.

En el directorio **/bin** se encuentran las shells y las utilidades (p. ej. **mount**) y un conjunto de utilidades para ficheros y red, como p. ej. **e2fsck**, que sirven para comprobar y arreglar sistemas de fichero. En **/sbin** se encuentran también los binarios más importantes para la administración del sistema como **fdisk**, **mkfs**, **mkswap**, **init**, **shutdown** y para el uso de red **ifconfig**, **route** y **netstat**.

En **/usr/bin** se encuentra el editor **vi** al igual que las herramientas (**grep**, **find**, **less**, etc.) y también **telnet**.

Acceso al sistema "normal"

Como punto de montaje del sistema SuSE Linux en el disco duro, está previsto el directorio **/mnt**, lo que no impide generar otros directorios y usarlos como puntos de montaje.

Supongamos que el sistema normal contiene según `/etc/fstab` las particiones Linux, como se observa en el ejemplo del fichero 25.

<code>/dev/sdb5</code>	<code>swap</code>	<code>swap</code>	<code>defaults</code>	<code>0</code>	<code>0</code>
<code>/dev/sdb3</code>	<code>/</code>	<code>ext2</code>	<code>defaults</code>	<code>1</code>	<code>1</code>
<code>/dev/sdb6</code>	<code>/usr</code>	<code>ext2</code>	<code>defaults</code>	<code>1</code>	<code>2</code>

Fichero 25: Ejemplo de `/etc/fstab`

Aviso

En el siguiente apartado vigile el orden en el que se han de montar los dispositivos.

Aviso

Para tener acceso a todo el sistema hay que montarlo paso por paso mediante `/mnt` con los siguientes comandos:

```
tierra:/ # mount /dev/sdb3 /mnt
tierra:/ # mount /dev/sdb6 /mnt/usr
```

Ahora se tiene acceso a todo el sistema y se pueden corregir errores en los ficheros de configuración como en `/etc/fstab`, `/etc/passwd` o `/etc/inittab`. Estos ficheros se encuentran ahora en `/mnt/etc` y no en `/etc`.

Es posible recuperar particiones totalmente perdidas, creándolas nuevamente con `fdisk`. Esto sólo funciona si se conoce con exactitud la posición en la que se encontraban antes en el disco duro. Por eso se recomienda guardar un impreso del fichero `/etc/fstab` y del resultado del comando:

```
tierra:~ # fdisk -l /dev/<disk>
```

En lugar de `<disk>` hay que indicar uno por uno los nombres de dispositivo de los discos duros del sistema, p. ej. `hda`.

Arreglar sistemas de ficheros

Un sistema de fichero dañado es una razón seria para recurrir al sistema de rescate. Se produce p. ej. por no haber apagado correctamente el ordenador (en caso de corte de la electricidad) o por un cuelgue de sistema. No se puede arreglar un sistema de fichero durante el uso normal del ordenador y en "casos graves" ni siquiera se puede montar el sistema de fichero raíz y el arranque termina con el mensaje "kernel panic". En tal caso sólo queda la posibilidad del arreglo "desde fuera" con un sistema de rescate.

El sistema de rescate de SuSE Linux contiene las utilidades `e2fsck` y también `dumpe2fs` para el diagnóstico, lo que sirve para la mayoría de problemas. Generalmente en casos de emergencia no se puede acceder a la página man `e2fsck`, por lo que se encuentra impresa en el anexo C en la página 573.

Ejemplo: Cuando un sistema de fichero se resiste a su montaje debido a un *superbloque no válido*, lo más probable es que `e2fsck` fracase en el intento de arreglarlo. La solución es usar uno de los backups del superbloque, que se encuentran cada 8192 bloques (bloque 8193, 16385...) en el sistema de ficheros. Esto se puede hacer con el comando:

```
tierra:~ # e2fsck -f -b 8193 /dev/⟨Partición_Dañada⟩
```

La opción `-f` fuerza la comprobación del sistema de ficheros para evitar que `e2fsck` asuma que todo está en orden por el hecho de haber detectado la copia intacta del Súper-bloque.

Consolas virtuales

Linux es un sistema multitarea y multiusuario. Las ventajas que aportan estas características se agradecen incluso en un sistema PC con un solo usuario:

El modo texto ofrece 6 consolas virtuales, a las que se puede acceder mediante las combinaciones de teclas `(Alt) + (F1)` a `(Alt) + (F6)`.

La séptima consola está reservada para X11. Modificando el fichero `/etc/inittab` se puede disponer de más o de menos consolas.

Si estando en X11 desea trabajar en una consola virtual sin cerrar X11, pulse las combinaciones `(Control) + (Alt) + (F1)` a `(Control) + (Alt) + (F6)`. Para volver a X11, pulse `(Alt) + (F7)`.

Distribución del teclado

Para normalizar la distribución del teclado de los distintos programas, se han modificado los siguientes ficheros:

```
/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  
/usr/lib/joerc
```

Estas modificaciones sólo tienen efecto sobre las aplicaciones que leen los parámetros `terminfo` o sobre aquellas cuyos ficheros de configuración fueron modificados directamente (`vi`, `less`, etc.). Se recomienda adaptar otras aplicaciones que no sean de SuSE a estas definiciones.

Dentro del entorno X Windows se puede acceder a la tecla Compose ("Multi_key") mediante la combinación de teclas  +  (derecha); véase el comentario en `/usr/X11R6/lib/X11/Xmodmap`.

Configuración nacional – I18N/L10N

Dado el nivel de internacionalización de SuSE Linux, es muy flexible para la adaptación a necesidades locales. En términos técnicos: La internacionalización ("I18N") permite implementar extensiones locales ("L10N"). Las abreviaciones I18N y L10N reemplazan los términos *internationalization* y *localization*, mencionando siempre la letra inicial y final así como el número de caracteres que faltan entremedio.

La configuración se realiza mediante las variables `LC_*` que se definen en el fichero `/etc/sysconfig/language`. Aparte del idioma para la interfaz gráfica de los programas y sus mensajes, se configuran también las categorías *moneda*, *cifras*, *fecha y hora*, *el tipo de caracteres*, *el tipo de mensajes* y *el criterio de ordenar*. Todas estas categorías se pueden definir dentro del fichero `language` mediante una variable individual o de forma indirecta mediante una variable de un nivel más alto (véase página del manual de `locale` (`man 5 locale`)):

1. `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 determinan las categorías arriba mencionadas. A continuación se detalla el significado de las distintas variables.

Mediante el comando `locale` es posible consultar la configuración actual.

2. `RC_LC_ALL`: En caso de estar definido, esta variable sobrescribe los valores de las variables mencionadas en el apartado 1.
3. `RC_LANG`: Al no definir ninguna de las variables arriba mencionadas, ésta sirve de definición por defecto "Fallback". SuSE Linux por defecto solo define `RC_LANG` para que el usuario tenga más facilidad de introducir valores propios.
4. `ROOT_USES_LANG`: Una variable booleana de valor `yes/no`; al tener `no` `root` siempre trabaja en el entorno POSIX.

Las demás variables se determinan mediante el editor `sysconfig`.

El valor de estas variables se compone de la identificación para el idioma (ingl. *language code*), del país o territorio (ingl. *country code*), del juego de caracteres (ingl. *encoding*) y de la opción (ingl. *modifier*). Todas estas indicaciones se unen mediante caracteres especiales:

```
LANG=<language>[_<COUNTRY>].Encoding[@Modifier]
```

Algunos ejemplos

Idioma y país se deben definir juntos. La indicación del idioma sigue la norma ISO 639 (<http://www.evertype.com/egt/standards/iso639/iso639-1-en.html> y <http://www.loc.gov/standards/iso639-2/>) y los códigos de país están definidos en la norma ISO 3166 (http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html). Solo se puede seleccionar valores que encuentran su homólogo en un fichero de descripción dentro del directorio `/var/lib/locale`. Es posible crear ficheros de descripción a partir de los ficheros `/usr/share/i18n` usando `localedef`. De esta forma un fichero de descripción para `es_ES@euro`. UTF-8 se crea mediante:

```
tierra:~ # localedef -i es_ES@euro -f UTF-8 es_ES@euro.UTF-8
```

LANG=es_ES.ISO-8859-1

Esta es la forma de configurar el idioma alemán en Alemania con el juego de caracteres ISO-8859-1. Éste aún no incorpora el símbolo del Euro pero sigue siendo necesario para los programas que aún no han sido adaptados a la ISO-8859-15.

Por ejemplo el programa Emacs analiza la codificación del juego de caracteres (aquí ISO-8859-15).

LANG=es_ES@euro

Este es un ejemplo para la definición de una opción (euro). `es_ES@euro` es la configuración predeterminada de una instalación en alemán.

LANG=es_ES.UTF-8

El parámetro UTF-8 sirve para trabajar en una `xterm` con Unicode. Para iniciar un `xterm` con UTF-8 se recomienda crear un script sencillo llamado p. ej. `uxterm` (véase el fichero 26).

```
#!/bin/bash
export LANG=es_ES.UTF-8
xterm -fn \
'-Misc-Fixed-Medium-R-Normal--18-120-100-100-C-90-ISO10646-1' \
-T 'xterm UTF-8' $*
```

Fichero 26: uxterm para iniciar un xterm con Unicode

SuSEconfig lee las variables de `/etc/sysconfig/language` y escribe los valores en los ficheros `/etc/SuSEconfig/profile` y `/etc/SuSEconfig/csh.cshrc`.

`/etc/profile` lee el fichero `/etc/SuSEconfig/profile` (lo usa como fuente) y `/etc/csh.cshrc` lee `/etc/SuSEconfig/csh.cshrc`. De esta forma la configuración está disponible para todo el sistema.

La configuración del sistema puede ser modificada por los usuarios con el fichero de configuración individual de usuario `~/ .bashrc`. Por ejemplo, cuando la configuración del sistema es `es_ES` y el usuario prefiere los mensajes en inglés, es posible modificarlo mediante:

```
LC_MESSAGES=en_US
```

Configuración del idioma soportado

Los ficheros de la categoría *Mensajes* normalmente sólo se encuentran dentro del directorio de idioma (p. ej. `de`) para tener una solución de respaldo. Por ejemplo cuando el valor de `LANG` está en `de_AT` y el fichero de mensajes no se encuentra en `/usr/share/locale/de_AT/LC_MESSAGES`, entonces el fichero `/usr/share/locale/de/LC_MESSAGES` sirve de respaldo para los mensajes.

Otra posibilidad es la de definir una cadena de respaldos, p. ej. para bretón → francés o para español → gallego → portugués:

```
LC_MESSAGES="br_FR.ISO-8859-15:fr_FR.ISO-8859-15"
LC_MESSAGES="es_ES.ISO-8859-15:gl_ES.ISO-8859-15\
:pt_PT.ISO-8859-15"
```

O para – dependiendo de las preferencias – cambiar a las variantes noruegas “nyorsk” o bien “bokmål” (con fallback automático a `no`):

```
LANG="nn_NO"
LANGUAGE="nn_NO:nb_NO:no"
```

o

```
LANG="nb_NO"
LANGUAGE="nb_NO:nn_NO:no"
```

Con el noruego también hay que tener en cuenta que se trata `LC_TIME` de forma diferente.

Posibles problemas

- En cadenas de números no se reconoce el punto como separador de miles. Probablemente el valor de LANG esté en de. Como la descripción que usa la glibc se encuentra en /usr/share/locale/de_DE/LC_NUMERIC, LC_NUMERIC debe tener p. ej. el valor es_ES.

Información adicional:

- *The GNU C Library Reference Manual*, capítulo "Locales and Internationalization"; se encuentra dentro de paquete glibc-info.
- Jochen Hein ?, bajo la palabra clave "NLS".
- *Spanish-HOWTO* de Gonzalo García-Agulló <file:/usr/share/doc/howto/en/html/Spanish-HOWTO.html>
- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux*, actualizado en <http://www.cl.cam.ac.uk/~mgk25/unicode.html>.
- *Unicode-Howto* de Bruno Haible <file:/usr/share/doc/howto/en/html/Unicode-HOWTO.html>.

El concepto de arranque de SuSE Linux

El arranque e inicio de un sistema UNIX provoca un hormigueo incluso al administrador de sistemas más experimentado. Este capítulo es una breve introducción al concepto de arranque de SuSE Linux. La implementación actual de la iniciación del sistema utiliza la especificación LSB versión 1.3.x (véase el apartado *Linux Standard Base (LSB)* en la página 266).

El programa <code>init</code>	296
Los niveles de ejecución – “runlevels”	296
Cambio de nivel de ejecución	298
Los scripts de inicio	299
El editor de niveles de ejecución de YaST	303
SuSEconfig y <code>/etc/sysconfig</code>	304
El editor Sysconfig de YaST	306

Con las lapidarias palabras "Uncompressing Linux..." el Kernel toma las riendas de todo el hardware del sistema; comprueba y fija la consola – más exactamente el registro de la BIOS de la tarjeta gráfica y el formato de salida de la pantalla –, para después leer los valores predeterminados de la BIOS e iniciar las interfaces elementales de la placa base. En los próximos pasos los distintos controladores – que forman parte del kernel – "prueban" el hardware presente para iniciarlo en caso necesario. Después del "chequeo de la partición" y la carga del Root-Filesystem, el kernel ejecuta el `init`, el cual realiza el auténtico arranque del sistema con sus múltiples programas auxiliares y sus configuraciones. El kernel sigue gestionando el sistema completo, el tiempo de cálculo de los programas y los accesos al hardware.

El programa `init`

El programa `init` es el proceso encargado de iniciar correctamente el sistema, por lo que puede decirse que todos los procesos del sistema son "hijos" de `init`.

Dentro de todos los programas, `init` tiene una jerarquía especial: `init` es ejecutado directamente por el kernel y por lo tanto es inmune a la señal 9 con la cual todos los procesos pueden ser "interrumpidos". Los procesos siguientes son ejecutados directamente por `init` o por uno de sus "procesos subordinados".

`init` se configura de forma centralizada a través del archivo `/etc/inittab`; aquí se definen los llamados "niveles de ejecución" (ingl. *Runlevel*) (se comenta con más detalle en el apartado [Los niveles de ejecución – "runlevels"](#) en esta página) y se determina qué servicios y daemons deben estar disponibles en los diferentes niveles. Dependiendo de la escritura en `/etc/inittab`, `init` ejecuta diferentes scripts que por razones de organización se reúnen en el directorio `/etc/init.d`.

Así, todo el proceso de arranque – y naturalmente la secuencia de apagado – es controlado por el proceso `init`; en este sentido se puede considerar al kernel prácticamente como "proceso en segundo plano", el cual tiene como objetivo gestionar los procesos arrancados, dedicarles tiempo de cálculo y posibilitar y controlar el acceso al hardware.

Los niveles de ejecución – "runlevels"

Bajo Linux existen diferentes *runlevels* (niveles de ejecución), que definen qué estado debe tener el sistema. El nivel estándar, en el cual arranca el sistema, está recogido en el archivo `/etc/inittab` mediante `initdefault`; normalmente

es 3 o 5 (ver resumen en la tabla 12.1). Alternativamente se puede introducir el nivel de ejecución requerido en el proceso de arranque (p. ej. en el prompt de LILO); el kernel pasa los parámetros que no puede evaluar al proceso `init` sin modificarlos.

Se puede cambiar a otro nivel de ejecución introduciendo sólo `init` con el número correspondiente. Naturalmente, el cambio a otro nivel sólo puede ser gestionado por el administrador de sistema. Por ejemplo, con el comando `init 1` o `shutdown now` se logra entrar en el *modo monousuario* (ingl. *single user mode*), el cual se ocupa del mantenimiento y administración del sistema. Después de que el administrador del sistema haya acabado su trabajo, puede utilizar `init 3` para arrancar el sistema en el nivel de ejecución normal, en el cual se ejecutan todos los programas necesarios y los usuarios individuales pueden entrar al sistema. Con `init 0` o `shutdown -h now` se puede parar el sistema y con `init 6` o `shutdown -r now` reiniciarlo.

Atención

Nivel de ejecución 2 con la partición `/usr/` montada vía NFS

El nivel de ejecución 2 no debe utilizarse en sistemas en los que la partición `/usr/` haya sido montada vía NFS. La partición `/usr/` contiene programas muy importantes necesarios para manejar correctamente el sistema. Debido a que el servicio NFS todavía no está disponible en el nivel de ejecución 2 (modo multiusuario local sin red remota), las funciones del sistema estarían muy limitadas.

Atención

Nivel de ejecución	Significado
0	Parada de sistema (ingl. <i>system halt</i>)
S	Modo monousuario (ingl. <i>single user mode</i>); desde el prompt de arranque con distribución de teclado inglesa.
1	Modo monousuario (ingl. <i>Single user mode</i>)
2	Modo multiusuario local sin red remota (ingl. <i>local multiuser without remote network (e. g. NFS)</i>)
3	Modo multiusuario completo con red (ingl. <i>full multiuser with network</i>)
4	Libre (ingl. <i>Not used</i>)
5	Modo multiusuario completo con red y KDM (estándar), GDM o XDM (ingl. <i>full multiuser with network and xdm</i>)
6	Reiniciar el sistema (ingl. <i>system reboot</i>)

Cuadro 12.1: Lista de los niveles de ejecución disponibles en Linux

En una instalación estándar de SuSE Linux normalmente se configura el nivel de ejecución 5 como valor por defecto, de modo que los usuarios puedan entrar directamente al entorno gráfico del sistema. Si por un ajuste manual la configuración de nivel de ejecución 5 no se hubiera realizado, es posible efectuar posteriormente una reconfiguración.

Si quiere cambiar el valor del nivel de ejecución estándar de 3 a 5, tiene que asegurarse de que sistema X Window ya está correctamente configurado; (apartado [El sistema X Window](#) en la página 99) . Para comprobar que el sistema funciona de la forma deseada, introduzca `init 5`. En caso afirmativo, puede cambiar el nivel de ejecución por defecto mediante YaST al valor 5.

Aviso

Modificaciones en `/etc/inittab`

Un `/etc/inittab` alterado puede provocar que el sistema ya no arranque correctamente. Hay que tener mucho cuidado al modificar este archivo y no olvidarse de conservar siempre una copia del archivo intacto. – Para remediar el problema se puede intentar transferir el parámetro `init=/bin/sh` desde el prompt de LILO para arrancar directamente dentro de una shell y desde allí recuperar el archivo. Después del arranque, se puede recuperar la copia de seguridad con `cp`.

Aviso

Cambio de nivel de ejecución

En un cambio de nivel de ejecución suele ocurrir lo siguiente. Los llamados *scripts de parada* del nivel actual se ejecutan– los diferentes programas que se están ejecutando en este nivel se finalizan – y los *scripts de arranque* del nuevo nivel se inician. En un procedimiento como éste, en la mayoría de los casos se ejecutan varios programas.

Para que sea más claro, veamos en un ejemplo qué ocurre si cambiamos del nivel 3 al 5:

- El administrador (`root`) comunica al proceso `init` que debe cambiar el nivel de ejecución introduciendo `init 5`.
- `init` consulta el archivo de configuración `/etc/inittab` y detecta que el script `/etc/init.d/rc` debe ser ejecutado con el nuevo nivel de ejecución como parámetro.

- Ahora el programa `rc` ejecuta todos los scripts de parada del nivel actual para los cuales no existe un script de arranque en el nivel nuevo. En nuestro ejemplo son todos los scripts que se encuentran en el subdirectorio `/etc/init.d/rc3.d` (el último nivel de ejecución era 3) y que comienzan con la letra 'K'. El número que sigue a la 'K' asegura que se mantenga un cierto orden en el proceso, ya que algunos programas pueden depender de otros.

Atención

Los nombres de los scripts de parada comienzan siempre con 'K' (ingl. *kill*), los de los scripts de arranque con 'S' (ingl. *start*).

Atención

- Por último se llama a los scripts de arranque del nuevo nivel de ejecución. Éstos están en nuestro ejemplo en `/etc/init.d/rc5.d` y comienzan con una 'S'. También aquí se mantiene un orden determinado, el cual queda fijado por el número que sigue a la 'S'.

Si cambia al mismo nivel en el que se encuentra, `init` lee solamente el `/etc/inittab`, comprueba el archivo buscando cambios y en caso necesario realiza los procedimientos adecuados (p. ej. ejecuta un `getty` en otra interfaz).

Los scripts de inicio

Los scripts bajo `/etc/init.d` se dividen en dos categorías:

- scripts llamados *directamente* por `init`: Esto sólo sucede en el caso del arranque así como también en caso de un apagado instantáneo (en caso de un corte del suministro eléctrico o por pulsar el usuario la combinación de teclas `(Control) + (Alt) + (Supr)`).
- scripts llamados *indirectamente* por `init`: Esto ocurre en el caso de un cambio del nivel de ejecución; aquí generalmente se ejecuta el script superior `/etc/init.d/rc`, el cual se encarga de que los scripts correspondientes sean ejecutados en el orden correcto.

Todos los scripts se encuentran bajo `/etc/init.d`. Los que se usan para el cambio del nivel de ejecución se encuentran también en este directorio, pero son ejecutados siempre como un enlace simbólico desde uno de los subdirectorios `/etc/init.d/rc0.d` hasta `/etc/init.d/rc6.d`. Esto tiene fines organizativos y evita que los scripts tengan que estar presentes varias veces si son

utilizados en diferentes niveles. Para que cada uno de los scripts pueda ser ejecutado como script de arranque o de parada, éstos tienen que admitir los dos parámetros `start` y `stop`. Aparte de estos dos parámetros, los scripts son capaces de procesar las opciones `restart`, `reload`, `force-reload` y `status`, cuyo significado se explica con más detalle en la tabla 12.2.

Opción	Significado
<code>start</code>	Iniciar el servicio
<code>stop</code>	Parar el servicio
<code>restart</code>	Con el servicio en ejecución, pararlo y reiniciarlo; en caso contrario, iniciarlo
<code>reload</code>	Leer la configuración del servicio nuevamente sin parada y reinicio del servicio
<code>force-reload</code>	Leer nuevamente la configuración del servicio si este lo soporta; en caso contrario igual que <code>restart</code>
<code>status</code>	Mostrar estado actual

Cuadro 12.2: Resumen de las opciones de los scripts de inicio

Los enlaces en los subdirectorios específicos de los niveles de ejecución sólo sirven para unir cada script a un determinado nivel. Los enlaces necesarios se crean y se quitan mediante `insserv` (o mediante el enlace `/usr/lib/lsb/install_initd`) en el momento de instalar o desinstalar el paquete; ver página del manual de `insserv` (`man 8 insserv`).

A continuación se ofrece una breve descripción del primer script de arranque y del último script de parada, así como del script de control:

boot Este script es ejecutado directamente por `init` en el arranque del sistema, es independiente del nivel de ejecución requerido por defecto y se ejecuta sólo una vez. Fundamentalmente, se montan los volúmenes `proc` y `devpts`, se arranca el `blogd` y – después de la primera instalación o de una actualización – se ejecuta una configuración básica.

`blogd` es el primer daemon que inician `boot` y el script `rc` y vuelve a cerrarse una vez realizado el trabajo correspondiente (por ejemplo activar subscrips). Este daemon escribe en el archivo de registro `/var/log/boot.msg` en caso de que `/var` esté montado con permisos de lectura y escritura, o bien almacena temporalmente todos los datos de la pantalla hasta que `/var` se monta con permisos de lectura y escritura. Puede obtener información adicional sobre `blogd` en `man blogd`.

Adicionalmente, este script se hace cargo del directorio `/etc/init.d/boot.d`. Al arrancar el sistema se ejecutan en este directorio todos los

scripts cuyos nombres comienzan con 'S'. Se realiza la comprobación de los sistemas de archivos, se eliminan los archivos sobrantes en `/var/lock` y se configura la red para el Loopback-Device. Acto seguido se fija el tiempo real del sistema.

Si aparece un fallo grave durante la comprobación y reparación automática de los sistemas de archivo, el administrador del sistema tiene la posibilidad de resolver el problema manualmente después de haber introducido la contraseña de root. Por último se ejecuta el script `boot.local`.

boot.local Aquí se pueden introducir programas o servicios adicionales que deban ejecutarse en el arranque antes de que el sistema entre en uno de los niveles de ejecución. Por su función es equiparable al archivo `AUTOEXEC.BAT` de DOS.

boot.setup Opciones de configuración básicas que se deben realizar cuando se cambia desde el modo de usuario único a cualquier otro nivel de ejecución. Aquí se cargan la distribución del teclado y la configuración de la consola.

halt Este script sólo se ejecuta entrando en los niveles 0 o 6 y puede ejecutarse con el nombre `halt` o `reboot`. Dependiendo del nombre asignado a `halt`, el sistema se reinicia o se apaga totalmente.

rc Es el script superior, el cual es invocado en cada cambio del nivel de ejecución. Ejecuta los scripts de parada del nivel actual y a continuación los scripts de arranque del nuevo.

Añadir scripts init

Resulta muy fácil añadir scripts init adicionales al concepto descrito en las líneas superiores. Puede obtener información referente al formato, asignación de nombres y organización de los scripts init en el diseño del LSB así como en las páginas del manual de `init`, `init.d` e `insserv`. Las páginas del manual de `startproc` y `killproc` también le serán de gran ayuda.

Aviso

Elaboración de scripts de arranque propios: Los scripts defectuosos pueden provocar el bloqueo del ordenador. Tenga mucho cuidado a la hora de elaborar scripts propios y pruébelos tanto como le sea posible antes de ejecutarlos en un entorno multiusuario. Para más información básica sobre cómo manejar scripts de arranque y niveles de ejecución, vea el apartado *Los niveles de ejecución – "runlevels"* en la página 296.

Aviso

- Si desea crear un script init para un programa o servicio (ingl. *service*) propio, puede utilizar el archivo `/etc/init.d/skeleton` como plantilla. Guarde este archivo bajo un nombre nuevo y edite los nombres de programas o archivos y las rutas. Dado el caso también puede añadir al script nuevos componentes propios que sean necesarios para ejecutar correctamente el comando de inicio.
- Edite el bloque obligatorio `INIT INFO` al principio del archivo:

```
### BEGIN INIT INFO
# Provides:          F00
# Required-Start:    $syslog $remote_fs
# Required-Stop:     $syslog $remote_fs
# Default-Start:     3 5
# Default-Stop:      0 1 2 6
# Description:       Start F00 to allow XY and provide YZ
### END INIT INFO
```

Mensaje en pantalla 14: Bloque INIT INFO mínimo

En la primera línea de la cabecera `INFO`, a continuación de `Provides:`, se introduce el nombre del programa o servicio que va a controlarse por medio del script. En las entradas `Required-Start:` y `Required-Stop:` se incluyen todos los servicios que deben ser iniciados o terminados antes del inicio o parada del servicio o programa en cuestión. Esta información se analiza para generar la numeración de los scripts de arranque y parada resultantes en los directorios de niveles de ejecución. En las entradas `Default-Start:` y `Default-Stop:` se introducen los niveles de ejecución en los que la aplicación ha de iniciarse o detenerse automáticamente. Una breve descripción de la aplicación en `Description:` pone punto y final a este bloque.

- Utilice el comando `insserv <nombre_nuevo_script>` para crear los enlaces desde `/etc/init.d/` a los directorios de niveles de ejecución correspondientes (`/etc/init.d/rc?.d/`). `insserv` analiza automáticamente los datos introducidos en la cabecera del script init y guarda los enlaces para los scripts de arranque y parada en los directorios de niveles de ejecución respectivos. `insserv` también se encarga de mantener el orden de inicio y parada dentro de un nivel de ejecución mediante la numeración de los scripts.

El editor de niveles de ejecución de `YaST` constituye una herramienta gráfica para crear los enlaces; véase la sección *El editor de niveles de ejecución de YaST* en la página siguiente.

Si se trata únicamente de integrar un script ya existente en `/etc/init.d/` en el concepto de los niveles de ejecución, cree los enlaces a los directorios de niveles de ejecución respectivos con `insserv` o el editor de niveles de ejecución de YaST y active el servicio. La próxima vez que inicie el sistema, los cambios serán aplicados y el nuevo servicio se activará automáticamente.

El editor de niveles de ejecución de YaST

Al iniciar este módulo se abre una máscara resumen que muestra todos los servicios disponibles y su estado de activación. Un botón le permite seleccionar uno de los dos modos posibles, 'Modo sencillo' o 'Modo experto'. La opción predeterminada es 'Modo sencillo', la cual suele resultar suficiente para la mayoría de los casos de aplicación. Un resumen en forma de tabla muestra en orden alfabético todos los servicios y daemons disponibles en el sistema. En la columna de la izquierda aparece el nombre del servicio, en la columna central su estado de activación y a la derecha una breve descripción del mismo. Debajo de la tabla se muestra una descripción más larga del servicio seleccionado en ese momento. Para activar un servicio, selecciónelo en la tabla y pulse 'Activar'. Proceda de la misma forma para desactivar un servicio.

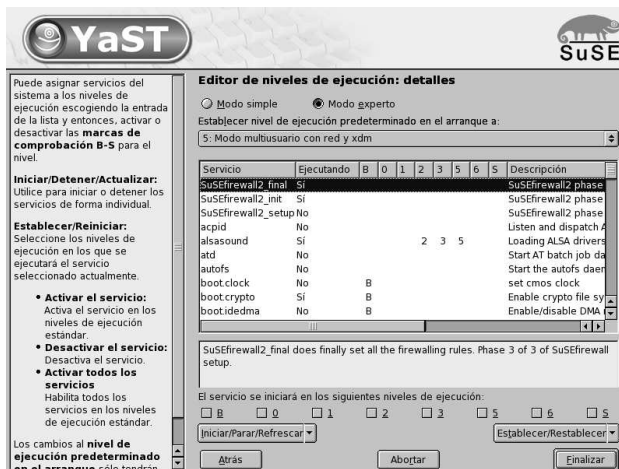


Figura 12.1: YaST: Editor de niveles de ejecución

Si desea controlar únicamente el nivel de ejecución en el que un servicio ha de iniciarse o detenerse, o cambiar el nivel de ejecución predeterminado, cambie

al ‘Modo experto’ por medio del botón. En la máscara que aparece a continuación se muestra primero el nivel de ejecución predeterminado. Este “modo de operación” es el que se inicia al arrancar el ordenador. El nivel predeterminado en SuSE Linux suele ser el número 5 (modo multiusuario completo con red y XDM). Otro nivel adecuado sería p. ej. el número 3 (modo multiusuario completo con red). YaST le permite definir en esta máscara otro nivel de ejecución predeterminado, ver tabla 12.1 en la página 297. La activación/desactivación de servicios y daemons se produce en la tabla resumen. Esta tabla le informa sobre qué servicios y daemons están disponibles, cuáles están activos en el sistema y en qué niveles de ejecución. Marcando una línea con el ratón puede activar una de las casillas ‘0’, ‘1’, ‘2’, ‘3’, ‘5’, ‘6’ y ‘S’ para determinar el nivel de ejecución en el que se debe iniciar el servicio en cuestión. El nivel de ejecución 4 se mantiene libre para una configuración individual del usuario. Justo debajo del resumen se ofrece una breve descripción del servicio o daemon seleccionado.

‘Iniciar’ y ‘Parar’ sirven para activar o desactivar un determinado servicio. ‘Actualizar’ comprueba el estado actual en caso de que no funcione automáticamente. ‘Valor por defecto’ representa la posibilidad de recuperar la configuración estándar (el estado posterior a la instalación del sistema). ‘Activar servicio’ sólo aparece si el servicio estuviera desactivado. ‘Configuración estándar para todos los servicios’ devuelve todos los servicios al estado original posterior a la instalación. ‘Terminar’ guarda esta configuración de sistema.

Aviso

Editar las configuraciones del Runlevel

La configuración defectuosa de los servicios del sistema y de los niveles de ejecución pueden provocar un fallo general en su sistema. Infórmese antes de realizar una modificación en las configuraciones de las posibles consecuencias, con el fin de proteger el funcionamiento del sistema.

Aviso

SuSEconfig y /etc/sysconfig

Gran parte de la configuración de SuSE Linux se puede realizar mediante los archivos de configuración en /etc/sysconfig. Las antiguas versiones de SuSE Linux utilizaban el archivo /etc/rc.config para la configuración del sistema. Este archivo es obsoleto y ya no se crea al realizar una nueva instalación de SuSE Linux. La configuración completa del sistema se lleva a cabo en los archivos situados en /etc/sysconfig. No obstante, el archivo /etc/rc.config ya existente se mantiene al actualizar.

A los archivos en `/etc/sysconfig` sólo se accede de forma puntual desde determinados scripts; de esta forma se garantiza que las configuraciones de red sólo sean utilizadas por los scripts de red. Además se pueden generar muchos más archivos de configuración del sistema dependientes de los archivos generados en `/etc/sysconfig`; de lo cual se encarga `/sbin/SuSEConfig`. Así p. ej., después de un cambio en la configuración de la red se genera de nuevo el archivo `/etc/host.conf`, puesto que depende del tipo de configuración.

Por tanto, si se realizan cambios en los archivos mencionados, se debe ejecutar posteriormente `SuSEConfig` para garantizar que la nueva configuración se aplique en todos los sitios relevantes. Este no es el caso si modifica la configuración con el editor `sysconfig` de `YaST`, ya que éste ejecuta automáticamente `SuSEConfig` con lo cual ya se actualizan los archivos correspondientes.

Este concepto permite realizar cambios fundamentales en la configuración del ordenador, sin necesidad de arrancar de nuevo; no obstante algunos cambios son muy profundos y, según las circunstancias, algunos programas tienen que ser arrancados nuevamente.

Si por ejemplo ha modificado la configuración de red, al ejecutar manualmente los comandos `rcnetwork stop` y `rcnetwork start` se consigue que los programas de red afectados se reinicien.

Se recomienda el siguiente procedimiento para la configuración del sistema:

- Ejecutar el comando `init 1` para cambiar el sistema al nivel de ejecución 1 "single user mode".
- Realizar los cambios requeridos en los archivos de configuración. Esto se puede hacer con un editor de texto o mejor con el editor de `sysconfig` de `YaST`; ver apartado *El editor Sysconfig de YaST* en la página siguiente.

Atención

Edición manual de la configuración del sistema

Si *no* utiliza `YaST` para editar los archivos de configuración en `/etc/sysconfig`, escriba los parámetros vacíos como dos signos sucesivos de comillas (p. ej. `<KEYTABLE="">`) y entrecomille también los parámetros que contengan espacios. Esto no es necesario para las variables formadas por una única palabra.

Atención

- Ejecutar `SuSEConfig` para realizar los cambios en los diferentes archivos de configuración. Esto ocurre automáticamente si las modificaciones se realizan con `YaST`.

- Devolver el sistema al nivel de ejecución anterior (3 en este ejemplo) mediante el comando `init 3`.

Este procedimiento sólo es necesario en caso de cambios amplios en la configuración del sistema (p. ej. configuración de la red). Para tareas sencillas de administración no es necesario entrar en el "single user mode"; sin embargo, así se asegura que todos los programas afectados por las modificaciones arranquen de nuevo.

Truco

Para desconectar por completo la configuración automática vía `SuSEconfig`, se puede activar la variable `<ENABLE_SUSECONFIG>` en `/etc/sysconfig/suseconfig` dándole el valor `no`. Si quiere recurrir al soporte de la instalación, debe dar el valor `yes` a la variable `<ENABLE_SUSECONFIG>`. También es posible deshabilitar la configuración automática selectivamente.

Truco

El editor Sysconfig de YaST

En el directorio `/etc/sysconfig` se encuentran los archivos que contienen las configuraciones más importantes de SuSE Linux (antiguamente gestionadas desde el archivo `/etc/rc.config`). El editor Sysconfig de YaST muestra un resumen de todas las posibilidades de configuración. Se pueden modificar los valores para pasarlos posteriormente a los archivos de configuración que los albergan. Por lo general no hace falta realizar este tipo de modificación manualmente, ya que cuando un paquete se instala o se configura un determinado servicio, los archivos se modifican automáticamente.

Aviso

Modificaciones en los archivos `/etc/sysconfig/*`

No se deben realizar modificaciones en `/etc/sysconfig/*` sin tener suficiente conocimiento previo, ya que partes importantes del sistema podrían dejar de funcionar. Todas las variables sysconfig de los archivos `/etc/sysconfig/` incluyen breves comentarios donde se documenta la función de la variable en cuestión.

Aviso

El editor sysconfig de YaST se inicia con una ventana dividida en tres partes. En la parte izquierda aparece una vista de árbol en la que puede seleccionarse la

variable que se va a configurar. Una vez seleccionada la variable, aparece en la ventana de la derecha el nombre de la selección y la configuración actualmente activa de esa variable. Por debajo de la variable se muestra una breve descripción de la misma, sus valores posibles, el valor por defecto y los archivos en los que se almacena esta variable. La máscara incluye además qué script de configuración se ejecutará en caso de modificar esta variable y qué servicio será reiniciado. YaST le pide una confirmación de los cambios y le informa de los scripts que deben ser ejecutados tras abandonar el módulo con 'Finalizar'. También tiene la posibilidad de saltarse el inicio de determinados servicios y scripts si todavía no desea iniciarlos.

Parte IV

La red

Fundamentos de conexión a redes

Linux, que de hecho nació en Internet, proporciona todas las herramientas y prestaciones de red necesarias para la integración en estructuras de red de todo tipo.

A continuación se expone una introducción al protocolo de red TCP/IP - normalmente utilizado por Linux - con sus características y particularidades.

Después de los fundamentos se explica cómo configurar una tarjeta de red mediante YcST. Se explica el significado de los ficheros de configuración más importantes y algunas de la herramientas más comunes.

Puesto que la configuración de una red puede llegar a ser muy compleja, en este capítulo sólo le explicaremos los conceptos más fundamentales.

Con YcST también puede configurar cómodamente la conexión a Internet vía PPP, módem, RDSI o DSL, lo cual se explica en *Manual del usuario*.

TCP/IP - El protocolo de red utilizado por Linux	312
IPv6 – La próxima generación de Internet	320
El acceso a la red	326
Configuración manual de la red	329
Routing en SuSE Linux	337
DNS – Domain Name System	339
El servicio de directorio LDAP	351
NIS – Network Information Service	377
NFS – Sistema de archivos distribuidos	382
DHCP	387
Sincronización horaria con xntp	392

TCP/IP - El protocolo de red utilizado por Linux

Linux utiliza al igual que otros sistemas operativos un protocolo de comunicación que se llama TCP/IP. En realidad no se trata de un solo protocolo de red sino de una familia de protocolos con diferentes prestaciones. TCP/IP se desarrolló a base de una aplicación militar y su especificación actual se fijó en el año 1981 en un documento RFC (ingl. *Request for comments*). Los RFC son documentos que describen los diferentes protocolos de Internet y la implementación de ellos en un sistema operativo o en aplicaciones. Estos documentos se encuentran en Internet en la dirección <http://www.ietf.org/>. Desde 1981 el protocolo sólo se ha modificado en algunos detalles; la base del protocolo sigue siendo la misma.

Truco

Los documentos RFC describen la estructura de los protocolos de Internet. Para profundizar sobre un determinado protocolo, en el documento RFC del protocolo concreto, encuentra una fuente de información muy buena; consulte <http://www.ietf.org/rfc.html>

Truco

Para el intercambio de datos vía TCP/IP entre dos ordenadores con Linux, existen los servicios que se mencionan en la tabla 13.1 en la página siguiente:

Protocolos	Descripción
TCP	(ingl. <i>Transmission control protocol</i>) es un protocolo asegurado orientado a la conexión. Desde el punto de vista de las aplicaciones, los datos se transmiten como un caudal y es el sistema operativo que se encarga de convertirlos al formato adecuado para su transmisión. Las aplicaciones en la máquina remota reciben el caudal de datos tal como fue enviado y TCP se encarga de que el caudal llegue completo y ordenado. Por eso TCP se utiliza cuando el orden de los datos importa y cuando se puede hablar de una conexión.

Cuadro 13.1: Continúa en la página siguiente...

UDP	(ingl. <i>User Datagram protocol</i>) es un protocolo no asegurado y sin conexión. La transferencia de datos está orientada a paquetes que se creen directamente por parte de la aplicación. El orden de llegada de los paquetes no está garantizado y tampoco la llegada en sí. UDP sirve para aplicaciones que transmiten bloques de datos y tiene menos tiempo de respuesta que TCP.
ICMP	(ingl. <i>Internet control message protocol</i>) es un protocolo que básicamente no puede ser usado por el usuario, ya que su tarea es la de transmitir errores y de controlar los ordenadores que participan en el intercambio de datos. Además ICMP incorpora un modo especial de eco, que se puede comprobar mediante ping.
IGMP	(ingl. <i>Internet group management protocol</i>) es un protocolo que controla el comportamiento de los ordenadores utilizando IP-Multicast. Lamentablemente no se puede presentar este protocolo dentro del marco de este libro.

Cuadro 13.1: *Diferentes protocolos de la familia TCP/IP*

Todas las redes en el mundo que estén interconectadas vía TCP/IP, forman una sola red que se suele llamar Internet.

Casi todos los protocolos de hardware están basados en paquetes. Los datos a transmitir se han de dividir en pequeños "paquetes", ya que es imposible transmitirlos "de golpe".

TCP/IP también trabaja con paquetes, cuyo tamaño máximo es de casi 64 Kilo-byte. En realidad los paquetes suelen tener un tamaño mucho menor, ya que el tamaño máximo de un paquete sobre una Ethernet es de 1500 Byte. Por eso el tamaño de cada paquete TCP/IP se limita a estos 1500 Byte, cuando el paquete pasa por una red del tipo Ethernet. Para transmitir más datos, el sistema operativo tiene que enviar la cantidad correspondiente de paquetes.

Modelo de capas

Para ser exactos, el protocolo no se debería llamar TCP/IP sino sólo IP. Con IP (ingl. *Internet protocol*) no se asegura la transferencia. TCP (ingl. *Transmission control protocol*) es una capa de control por encima del protocolo IP, que garantiza la transmisión de los datos.

Finalmente el protocolo IP es superpuesto al protocolo que se encuentre por debajo y que depende directamente del hardware (p. ej. Ethernet). Los expertos hablan aquí de "modelo de capas". Compare la figura 13.1.

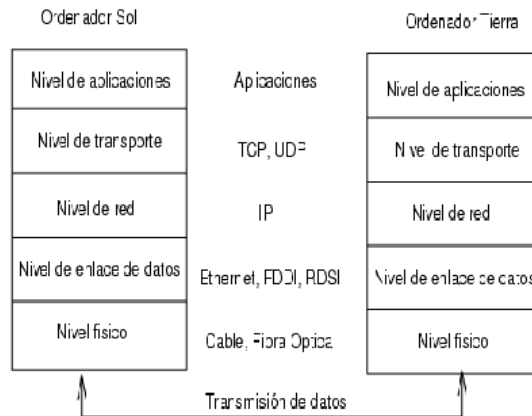


Figura 13.1: Modelo de capas simplificado para TCP/IP

La imagen muestra uno o dos ejemplos para cada capa. Las capas se ordenan según su nivel de abstracción; la capa inferior se encuentra más próxima al hardware, mientras que la capa superior "envuelve" el nivel de abstracción más alto. Cada capa tiene una determinada función que se explica a continuación. La función de cada capa se deduce en buena medida de su denominación. La red está representada por la capa de transmisión de bits y por la capa de seguridad.

- La primera capa se encarga de detalles como los tipos de cables, tipos de señales, la codificación de las mismas, etc y se denomina **Capa física**. La segunda capa se encarga del procedimiento de acceso a los datos y de la corrección de errores, por eso la capa se denomina **Capa de enlace**.
- La tercera capa es la **Capa de red** que se encarga de la transmisión de datos a distancia. Esta capa asegura que los datos encuentren el camino al destinatario a través de diversas redes.
- La **Capa de transporte** como cuarta capa se encarga de la llegada de los datos de las aplicaciones y del orden de los mismos. La capa de enlace

sólo asegura la llegada correcta de los datos, mientras que la capa de transporte evita la "pérdida" de estos.

- La quinta capa representa finalmente el procesamiento de datos por parte de la aplicación.

Cada capa necesita una cierta información adicional para poder cumplir con su tarea. Esta información se encuentra en el encabezado (ingl. *header*) de cada paquete. Cada capa añade un pequeño bloque de datos (denominado "cabeza de protocolo" (ingl. *Protocol header*)) al paquete que se está formando. La figura 13.2 muestra el ejemplo de la composición de un paquete TCP/IP que viaja sobre un cable de una red tipo Ethernet.

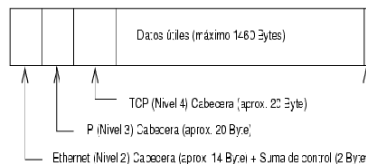


Figura 13.2: Paquete TCP/IP sobre Ethernet

Una excepción de la estructura del encabezado son los dígitos de control que no se encuentran en el encabezado sino al final. De esta forma el hardware de red lo tiene más fácil. Como se puede observar, el máximo útil de datos en un paquete sobre una red Ethernet es de 1460 Bytes.

Cuando una aplicación quiere enviar datos por la red, los datos pasan por las diferentes capas que se encuentran (con excepción de la primera) implementadas en el kernel de Linux. Cada capa se encarga de preparar los datos de tal forma que puedan ser pasados a la capa inferior. La capa más baja se encarga finalmente del envío de los datos.

Al recibir los datos, todo el proceso se invierte. Similar al proceso de pelar una cebolla, cada capa separa los encabezados de la parte útil de datos. Finalmente la cuarta capa se encarga de preparar los datos para la aplicación en la máquina remota.

Durante el proceso de transferencia, cada capa solo se comunica con aquella que se encuentra directamente encima o por debajo. Por eso para una aplicación es totalmente irrelevante si los datos viajan a través de una red de 100 MBit/s-FDDI o a través de una línea de módem de 56 kbit/s. Igualmente para la línea no son importantes los datos que se han de transferir sino que estos estén correctamente empaquetados.

Dirección IP (binario):	11000000	10101000	00000000	00010100
Dirección IP (decimal):	192 .	168 .	0 .	20

Cuadro 13.2: Formas de anotar una dirección IP

Direcciones IP y routing

Direcciones IP

Cada ordenador en Internet dispone de una dirección IP única de 32 bits. Estos 32 bits o bien 4 byte se representan normalmente como se muestra en la segunda fila de la tabla 13.2.

Como se puede observar, los cuatros bytes se anotan en el sistema decimal como cuatro cifras de 0 a 255 separadas por un punto. Esta dirección asignada al ordenador o a su interfaz de red es única y no puede ser utilizada en ningún otro lugar del mundo. Hay excepciones, pero estas no tienen relevancia en el ejemplo expuesto.

La tarjeta Ethernet por sí misma tiene un número único llamado MAC (ingl. *Media access control*). Este número es de 48 bit y único en el mundo; su fabricante lo almacena de forma fija en la tarjeta red. La asignación de los números MAC por parte de los fabricantes tiene una desventaja fatal: No hay ninguna jerarquía entre las tarjetas, sino que están distribuidas "al azar". Por eso no es posible utilizarlas para comunicarse con un ordenador a mucha distancia. Sin embargo la dirección MAC es de mucha importancia en una red local (es la parte importante de la cabeza del protocolo en la capa 2).

Volviendo a las direcciones IP: Los puntos separadores ya indican la estructura jerárquica de las direcciones. Hasta mediados de los noventa, había una separación estricta en clases. Este sistema resultó muy poco flexible por lo que se ha dejado de utilizar. Ahora se usa "routing sin clases" (CIDR (ingl. *classless inter domain routing*)).

Routing y máscaras de red

Puesto que los ordenadores con la dirección IP 192 . 168 . 0 . 20 no pueden saber dónde se encuentra la máquina con la dirección IP 192 . 168 . 0 . 1, se crearon las máscaras de red.

Simplificando se puede decir que la máscara de (sub-)red define para una computadora lo que se encuentra "fuera" y lo que se encuentra "dentro". Se puede acceder directamente a aquellos ordenadores que se encuentren "dentro" (dentro de la misma sub-red) mientras que a las máquinas que estén "fuera" solo se

Dirección IP: 192.168.0.20	11000000	10101000	00000000	00010100
Máscara de red: 255.255.255.0	11111111	11111111	11111111	00000000
Resultado binario	11000000	10101000	00000000	00000000
Resultado decimal	192.	168.	0.	0
Dirección IP: 213.95.15.200	11010101	10111111	00001111	11001000
Máscara de red: 255.255.255.0	11111111	11111111	11111111	00000000
Resultado binario	11010101	10111111	00001111	00000000
Resultado decimal	213.	95.	15.	0

Cuadro 13.3: Conjunción de direcciones IP con una máscara de red

llega a través de un enrutador (ingl. *router*) o una pasarela (ingl. *gateway*). Como cada interfaz de red recibe una IP propia todo puede llegar a ser muy complejo.

Antes de que un paquete empiece a tomar rumbo por la red, el ordenador realiza lo siguiente: Una conjunción bit por bit de la dirección de destino con la máscara de red (operación lógica Y) y de la dirección del remitente con la máscara (ver tabla 13.3). Si hay varias interfaces de red a disposición, se comprueban todas las direcciones de remitente posibles.

Los resultados de las conjunciones se comparan; en caso de que fueran idénticas, la máquina remota se encuentra en la misma subred que la máquina local. En cualquier otro caso hace falta acceder al ordenador remoto a través de una pasarela. Es decir, por más bits con valor "1" que se encuentren en la máscara de red, más ordenadores se accederán a través de la pasarela y menos se encontrarán en la propia subred. Para su explicación, la tabla 13.3 contiene un par de ejemplos.

La máscara de red se anota – tal como la dirección IP – con valores decimales separados por puntos. Esta máscara es también un valor de 32 bit y por eso se anotan igualmente en forma de cuatro cifras de tres dígitos cada una.

El usuario se encarga de definir qué ordenadores trabajan como pasarelas y a qué rangos de direcciones se accede mediante qué interfaces de red.

Un ejemplo práctico son todas las máquinas que se encuentran conectadas al mismo cable Ethernet.

Estas se encuentran entonces por lo general *en la misma subred* y se pueden acceder directamente. Igualmente si la Ethernet está dividida por switches o bridges, hay acceso directo a todos estos ordenadores.

Para atravesar distancias largas, ya no se puede utilizar la Ethernet económica, sino que hace falta pasar los paquetes IP por un soporte diferente (p. ej. FDDI o

RDSI). Tales aparatos se denominan router (enrutador) o gateway (pasarela). Un ordenador con Linux también se puede encargar de esto; la funcionalidad que lo realiza se denomina `ip_forwarding`.

En caso de trabajar con una pasarela, el paquete IP se manda a ésta y la pasarela trata de pasar el paquetes según el mismo esquema. Este proceso se repite hasta el momento de alcanzar el ordenador de destino o hasta que el “tiempo de vida del paquete” TTL (ingl. *time to live*) se haya agotado.

Tipo de direcciones	Descripción
La dirección base	Es la dirección de la máscara de red operada con la conjunción lógica AND (Y) con cualquier dirección de la red. Es exactamente lo que se refleja en la tabla 13.3 en la página anterior como Resultado de la conjunción . No se puede asignar esta dirección a ningún ordenador.
La dirección broadcast	Con esta dirección se puede contactar con todas las computadoras de la subred al mismo tiempo. La dirección se crea invirtiendo su valor binario y realizando una OR lógica con la dirección base de la red. En el caso del ejemplo mencionado resulta el valor 192.168.0.255. Esta dirección tampoco puede ser asignada a ninguna computadora.
Localhost	En cada ordenador la dirección 127 . 0 . 0 . 1 corresponde al dispositivo “Loopback”. La dirección sirve para crear una conexión en la propia máquina.

Cuadro 13.4: Direcciones especiales

No se pueden utilizar direcciones IP al azar, ya que estas deben ser únicas en todo el mundo. Para configurar un red privada con direcciones IP existen tres rangos de direcciones que pueden ser utilizados sin problema. Como desventaja, no es posible realizar con estas direcciones una conexión directa a Internet sin realizar algunas conversiones.

Los tres rangos reservados en RFC 1597 son los siguientes:

Red, máscara de red	Rango
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

Cuadro 13.5: Rangos para direcciones IP privadas

Domain Name System

DNS

Gracias al DNS no hace falta recordar direcciones IP, ya que este sistema realiza la asignación de una dirección IP a uno o varios nombres así como la asignación inversa de un nombre a una dirección IP. En Linux, un software especial llamado `bind` es el que se encarga de establecer el vínculo entre nombres y direcciones IP. Un ordenador que presta este servicio se denomina **Servidor de nombres** (ingl. *Nameserver*).

Los nombres también están estructurados dentro de una jerarquía; las diferentes partes funcionales de los nombres se separan por puntos. Esta jerarquía de nombres es independiente de la ya mencionada jerarquía de direcciones IP.

A continuación figura el ejemplo de un nombre completo:

`laurent.suse.de` descrito en formato `nombre_ordenador.dominio`. Un nombre completo se denomina "Nombre de dominio totalmente cualificado" (ingl. *Fully qualified domain name o FQDN*) y se compone del nombre del ordenador y de la parte del dominio. Este nombre de dominio se compone de una parte de libre elección – en el ejemplo `suse` – y del "dominio de primer nivel" (ingl. *Top level domain TLD*).

Por razones históricas la asignación de los TLDs no es del todo contundente. En los EE.UU. se utilizan TLDs de tres letras mientras que el resto del mundo utiliza los códigos de país ISO de dos letras.

En los primeros tiempos de Internet (antes de 1990) el fichero `/etc/hosts` albergaba los nombres de todos los ordenadores disponibles en Internet. Esta forma de resolución de nombre se tornó poco práctica debido al rápido crecimiento de Internet. Por eso se diseñó una base de datos descentralizada, capaz de guardar los nombres de las máquinas de forma distribuida.

Esta base de datos, representado por un servidor de nombres, no dispone de los datos de todas los ordenadores en Internet, sino que es capaz de consultar otros servidores de nombres en un nivel más alto.

En la punta de la jerarquía de servidores de nombres se encuentran los "Root-Nameserver" que administran los dominios de primer nivel (TLD). El "Network Information Center" (NIC) se encarga de la administración de estos servidores. El Root-Nameserver conoce los servidores de nombres que se encargan de cada dominio de primer nivel. En el caso de la TLD de Alemania (de) es DE-NIC que se encarga de todos los dominios de este tipo. En la página web <http://www.denic.de> hay más información sobre DE-NIC; <http://www.internic.net> informa sobre el NIC.

El ordenador de sobremesa tiene que conocer la dirección IP de al menos un servidor de nombres para que sea capaz de convertir nombres en direcciones IP. Con YcST es muy fácil configurar el servidor de nombres. En el caso de una conexión vía módem, puede que no sea necesario configurarlo manualmente, ya que el protocolo utilizado para la conexión proporciona esta información durante el proceso de conexión.

DNS es capaz de realizar otras tareas a parte de la resolución de nombres. El servidor de nombres "conoce" igualmente el ordenador que acepta los mensajes de todo un dominio. Este ordenador se conoce como "Mail exchanger (MX)".

El apartado *DNS – Domain Name System* en la página 339 explica la configuración de un servidor de nombres en SuSE Linux.

whois

El protocolo **whois** es muy similar al de DNS y sirve para averiguar rápidamente quién se responsabiliza de un determinado dominio.

IPv6 – La próxima generación de Internet

El por qué del nuevo protocolo de Internet

Debido a la aparición de la WWW (ingl. *World Wide Web*), Internet y la cantidad de ordenadores que se comunican vía TCP/IP han crecido vertiginosamente. Desde la invención de la WWW por parte de Tim Berners-Lee, que trabajaba en el CERN (<http://public.web.cern.ch/>) en el año 1990, la cantidad de los hosts en Internet ha crecido de algunos miles hasta alrededor de 100 millones, actualmente.

Como ya sabemos, una dirección IP "sólo" tiene 32 bits. Muchas de las direcciones IP se pierden por su estructuración. Internet se divide en subredes. Cada subred dispone de 2 elevado a N - 2 direcciones. Por eso una subred se compone por ejemplo de 2, 6, 14, 30, etc. direcciones IP. Para conectar p. ej. 128 ordenadores a Internet, se necesita una subred de "clase C" con 256 direcciones IP de

las que hay 254 útiles. Hay que restar dos direcciones para la dirección base de la red y para la de broadcast.

La configuración de un ordenador dentro de una red TCP/IP es relativamente complicada. Como se acaba de mencionar, hace falta configurar los siguientes parámetros en el ordenador: La dirección IP propia, la máscara de subred, la dirección de la pasarela (si existe) y el servidor de nombres. Es preciso conocer exactamente estos valores (p. ej. dados por parte del proveedor), ya que no se pueden deducir.

Cada paquete IP incorpora unos dígitos de control que se han de comprobar y de calcular cada vez que un paquete pasa por un router. Por eso los routers muy rápidos necesitan mucha potencia de cálculo, lo cual los encarece.

Hay algunos servicios que se realizan hasta ahora mediante Broadcasts (p. ej. el protocolo de red SMB de Windows). Los ordenadores que no participan en este servicio están igualmente obligados a procesar los paquetes para finalmente ignorarlos. Es algo que puede provocar problemas en redes con alta demanda de velocidad.

El sucesor de IP, IPv6, resuelve todos estos problemas. La meta principal del desarrollo era una fuerte ampliación del rango de direcciones y la simplificación de la configuración de clientes de sobremesa (hasta llegar a su automatización). Este apartado denomina IPv4 o IP al protocolo de Internet utilizado hasta la fecha, e IPv6 al protocolo de la nueva versión 6.

RFC 1752 expone los detalles de IPv6. La característica principal de IPv6 son las direcciones de 128 bits, que permiten muchos billones de direcciones. Con esta enorme cantidad es posible "permitirse el lujo" de definir como subred más pequeña una red de 48 bits.

De esta forma se puede utilizar la dirección MAC como una parte de la dirección. Como la MAC es única en el mundo, configurada por parte del fabricante, la configuración se simplifica mucho. En realidad los primeros 64 bits forman un "EUI-64-Token". Los últimos 48 bits vienen de la dirección MAC y los restantes 24 bits contienen información especial, que informa sobre el tipo de Token. Así es posible asignar EUI-64-Token a los dispositivos sin dirección MAC (en caso de conexiones por RDSI o PPP).

IPv6 incorpora una innovación: Se suele asignar a cada interfaz de red varias direcciones IP. La ventaja es que así se tiene directamente acceso a varias redes. Una de estas redes se puede formar con la dirección MAC y un prefijo conocido. Con esta red configurada automáticamente, se puede acceder a todos los ordenadores dentro de la red local, inmediatamente después del inicio de IPv6, utilizando la dirección "Link-local".

El resto de la configuración de un cliente también puede automatizarse. Para ello existe un protocolo especial para configurar los clientes en una red. Estos reciben su dirección IP desde un router.

Es muy importante que todos los ordenadores que trabajen con IPv6 soporten "Multicast". Multicast permite acceder simultáneamente y de forma selectiva a un grupo de ordenadores. No se accede a todos "de golpe" (broadcast) y tampoco a uno solo (unicast), sino a un determinado grupo. El grupo para acceder depende de la aplicación. Hay algunos grupos totalmente definidos como "todos los servidores de nombres" (ingl. *all nameservers multicast group*), o "todos los enrutadores" (ingl. *all routers multicast group*).

Existe un modo de compatibilidad, ya que no sería posible cambiar en un solo momento todos los ordenadores en Internet, de IPv4 a IPv6. Este modo traduce las direcciones actuales a las nuevas IPv6. A parte de esto existen mecanismos como "Tunneling" (paquetes del tipo IPv6 se envían dentro de un paquete IPv4). También es posible convertir direcciones IPv6 en direcciones IPv4, pero para acceder a un ordenador IPv6 desde una con IPv4 hace falta que la máquina con IPv6 tenga una dirección de compatibilidad con IPv4.

Estructura de una dirección IPv6

Es fácil de imaginar que la dirección IPv6 por sus 128 bits (16 Bytes) resulta mucho más larga que la IPv4 con apenas 32 bits.

Debido a su tamaño, las nuevas direcciones del tipo IPv6 se anotan en una forma distinta a las del tipo IPv4. Esto se ve reflejado en los ejemplos de la tabla 13.6 en la página siguiente.

Como se puede ver en la tabla, las direcciones IPv6 se representan mediante cifras hexadecimales. Éstas siempre se reúnen en grupos de dos bytes separadas por un : (dos puntos). Por esta razón cada dirección tiene un máximo de ocho grupos y siete doble puntos. Es permitido suprimir bytes de cero por delante, pero no en medio ni al final de un grupo. Es posible saltarse más de cuatro bytes de cero sucesivos utilizando el comodín :: (doble dos puntos). No se permite utilizar más de un comodín en una dirección. El proceso de suprimir los ceros se denomina en inglés "collapsing". Las direcciones compatibles con IPv4 tienen

Descripción	Valor de la dirección
Localhost	::1
Dirección IPv6 compatible IPv4	::10.10.11.102 (IPv6 está soportado)
Dirección IPv6 mapeado a IPv4	::ffff:10.10.11.102 (IPv6 no está soportado)
Dirección en general	3ffe:400:10:100:200:c0ff:fed0:a4c3
Dirección Link-local	fe80::10:1000:1a4
Dirección Site-local	fec0:1:1:0:210:10ff:fe00:1a4
Grupo Multicast	ff02:0:0:0:0:0:0:2
"todos los routers locales"	

Cuadro 13.6: *Diferentes direcciones IPv6*

una forma especial: La dirección IPv4 se añade sencillamente al prefijo definido para las direcciones compatibles IPv4.

Cada parte de una dirección IPv6 tiene un determinado significado. Los primeros bytes forman un prefijo que indica el tipo de la dirección. La parte del medio representa una red o bien no representa nada y el final de la dirección es la parte del host.

La tabla 13.7 en la página siguiente muestra el significado de algunos prefijos que se utilizan con frecuencia.

Prefijo (hexadecimal)	Uso
00	Direcciones IPv4 y <i>IPv4 compatibles sobre IPv6</i> . Son direcciones compatibles con IPv4. Un router adecuado tiene que convertir el paquete IPv6 en IPv4. Hay otras direcciones especiales (p. ej. Loopback Device) que utilizan este prefijo.
primera cifra 2 o 3	(ingl. <i>Aggregatable Global Unicast Address</i>). Igual que ahora, también en el caso de IPv6 se puede recibir la asignación de subredes a través de un proveedor.
fe80::/10	(ingl. <i>link-local</i>) Direcciones con este prefijo no pueden ser ruteadas y por tanto solo se pueden acceder en la misma subred.

Cuadro 13.7: *Continúa en la página siguiente...*

<code>fec0::/10</code>	(ingl. <i>site-local</i>) Estas direcciones pueden ser ruteadas, pero solamente dentro de una misma organización. Estas direcciones corresponden a las direcciones "privadas" actuales (p. ej. <code>10.x.x.x</code>).
<code>ff</code>	(ingl. <i>multicast</i>) Las direcciones IPv6 que comienzan con <code>ff</code> son direcciones Multicast.

Cuadro 13.7: *Diferentes prefijos IPv6*

Como se puede observar, especialmente las direcciones Unicast llegan a ser muy largas y es muy difícil memorizarlas. Por eso el buen funcionamiento del servidor de nombres es para IPv6 aún más importante que para IPv4.

Debido a la importancia del servidor de nombres existe un programa especial para la autoconfiguración del mismo.

Máscaras de red en IPv6

La representación de las máscaras de red en IPv6 es un poco diferente. La separación de las redes en clases carece de sentido, ya que desde un principio el enrutamiento es independiente de las clases de red y la subred más pequeña ya puede albergar una cantidad enorme de máquinas. Como las máscaras de red pueden llegar a ser muy largas, la anotación de las mismas es ahora muy diferente. En el siguiente número:

`fec0:1:1:0:210:10ff:fe00:1a4/64`

los últimos 64 bits forman la parte de host y los primeros 64 bits la parte de la red.

La cifra 64 significa que la máscara de red se rellena bit por bit comenzando en la izquierda. Por eso la máscara de red tiene 64 bits. Igual que en el caso de IPv4, una conjunción del tipo "Y" de la máscara de red con la dirección IP determina si el ordenador se encuentra en la misma subred o en otra.

Literatura y enlaces sobre IPv6

El resumen de IPv6 presentado no pretende ser una introducción completa acerca del amplio tema IPv6. Para más información, ver la literatura y libros online que se presenta a continuación:

<http://www.bieringer.de/linux/IPv6/> CÓMOs de IPv6 en Linux y muchos enlaces.

<http://www.6bone.de/> Acceder a IPv6 a través de un túnel.

<http://www.ipv6.org/> Todo acerca IPv6.

RFC 1725 El RFC introductorio sobre IPv6.

El acceso a la red

Finalmente TCP/IP se ha impuesto como el protocolo de red estándar y todos los sistemas operativos modernos son capaces de comunicarse con este protocolo. Sin embargo Linux sigue soportando otros protocolos de red como p. ej. IPX usado (anteriormente) por Novell Netware y Appletalk utilizado por los Macintosh. Este capítulo sólo explica la integración de un ordenador con Linux en una red TCP/IP.

La configuración de tarjetas de red "exóticas" como Arcnet, Token-Ring o FDDI se explica en la documentación de las fuentes del kernel en `/usr/src/linux/Documentation`. Desde SuSE Linux 8.0, las modificaciones en la configuración de redes se encuentran documentadas en el siguiente archivo: `/usr/share/doc/packages/sysconfig/README`.

Preparativos

El ordenador debe disponer de una tarjeta red soportada. Normalmente ésta se reconoce durante la instalación y el controlador adecuado se activa. El reconocimiento correcto de la tarjeta se nota entre otras cuando el resultado del comando `ifstatus eth0` muestra el dispositivo de red `eth0`.

Por defecto el kernel de SuSE realiza el soporte de la tarjeta de red mediante un módulo. En este caso el nombre del módulo debe aparecer como alias en el archivo `/etc/modules.conf`. Para la primera tarjeta Ethernet p. ej. de la siguiente forma: `alias eth0 tulip`

Esto funciona automáticamente cuando se carga durante la primera instalación desde `linuxrc` el controlador de la tarjeta de red. Posteriormente se puede realizar esta tarea con YaST.

Las tarjetas de red que soportan hotplug (p. ej. PCMCIA o USB) proporcionarán automáticamente los controladores al insertarlas; por lo tanto no se debe configurar nada. Puede encontrar más detalles en el capítulo [Hotplug](#) en la página [203](#).

Configuración de red con YaST2

YaST permite la configuración rápida de la tarjeta de red. Escoja en Centro de control la opción 'Red/Dispositivos' y después 'Configurar tarjeta de red'. En este diálogo, puede integrar una tarjeta de red con 'Añadir'; con 'Retirar' se eliminará la configuración de la tarjeta correspondiente; y con 'Cambiar' se puede modificar la configuración de la tarjeta.

Active la opción ‘Hardware’ para modificar con ‘Editar’ los datos de hardware de una tarjeta de red ya configurada. Aparece un menú para la configuración del hardware tal como se refleja en la figura 13.3

YaST suele configurar y activar correctamente la tarjeta de red durante la instalación. Por eso normalmente sólo se requiere una configuración manual trabajando con más de una tarjeta de red o cuando la autodetección del hardware falla. En tal caso hay que seleccionar ‘Añadir’ para seleccionar un controlador nuevo.



Figura 13.3: Configuración de los parámetros de hardware

Este diálogo permite seleccionar el tipo de tarjeta de red y, en caso de las tarjetas tipo ISA, también la interrupción y la dirección de entrada y salida (IO). Algunos controladores admiten parámetros especiales como la selección de la interfaz entre el conector RJ - 45 o el del tipo BNC. Para averiguarlo, consulte la documentación del controlador. Para PCMCIA y USB basta con activar las casillas correspondientes.

Después de haber introducido los parámetros de hardware, se pueden configurar los parámetros adicionales de la interfaz de red. Dentro del diálogo de la ‘Configuración básica de red’ seleccione el botón ‘Interfaz’ para activar la tarjeta recientemente configurada y para asignarle una dirección IP. Después de haber elegido la tarjeta pulse sobre ‘Editar’. Aparece un nuevo diálogo que permite asignar la dirección IP y definir datos adicionales de la red IP. Al configurar una red propia, se puede asignar las direcciones IP tal como lo expone el apartado 13 en la página 312 y la tabla 13.5 en la página 319.

Si no es así, los campos se han de rellenar con las direcciones asignadas por

parte del administrador de la red.

No olvide configurar un servidor de nombres en 'Hostname y nameserver' para que la resolución de nombres, tal como se explica en el apartado 13 en la página 339, funcione correctamente. La opción 'Routing' permite configurar el "routing" y mediante 'Configuración para expertos' se pueden realizar ajustes avanzados.

Si utiliza tarjetas de red inalámbricas, active la casilla 'Dispositivo wireless'. Ahora podrá llevar a cabo las configuraciones más importantes en el diálogo apropiado. En esencia estas son el modo de funcionamiento, el nombre de la red y la clave de codificación la transmisión de datos.

Aquí se termina la configuración de la red y YaST inicia SuSEconfig, que se encarga de introducir las indicaciones hechas en los correspondientes archivos. Para activar los ajustes y usar la nueva configuración hay que iniciar de nuevo los daemons correspondientes. Esto se consigue introduciendo el siguiente comando:

```
tierra:~ # rcnetwork restart
```

Hotplug/PCMCIA

Las tarjetas de red compatibles con hotplug, como p. ej. dispositivos PCMCIA o USB, son un caso especial dado que su denominación como dispositivo puede variar. Las tarjetas de red "fijas" siempre se identifican igual (p. ej. `eth0`) mientras que a este otro tipo se les asigna un nombre variable. Para evitar conflictos con tarjetas fijas, el servicio PCMCIA o hotplug se inicia siempre después de los servicios de red.

Por eso no hace falta iniciar los servicios PCMCIA antes de los servicios de red. Al contrario: Si estas tarjetas sólo fueran accionadas por el script de arranque de la red, existe la posibilidad de que se pierdan según avanza el funcionamiento del sistema.

Configurar IPv6

Para utilizar IPv6 normalmente no hace falta configurar nada especial en el lado de los clientes. Lo único que hace falta es cargar el soporte de IPv6 p. ej. mediante el comando

```
tierra:~ # modprobe ipv6
```

De acuerdo con la filosofía de autoconfiguración en IPv6, se asigna a la tarjeta una dirección de red dentro de la red `link-local`. Normalmente no se mantiene ninguna tabla de routing en un ordenador cliente, que puede consultar mediante el `Router Advertisement Protocol` los enrutadores que existen en la red y el prefijo que se ha de utilizar.

El programa `radvd` del paquete `radvd` sirve para configurar un enrutador IPv6. Este programa indica a los clientes el prefijo utilizado para las direcciones IPv6 y el/los router(s) en la red.

Es muy aconsejable instalar un enrutador con el programa `radvd` ya que éste realiza la asignación de las direcciones IPv6 de forma totalmente automática.

Configuración manual de la red

La configuración manual de la red no es muy aconsejable, ya que es más sencillo usar `YaST`.

Lo esencial aquí es que todas las interfaces de red estén redactadas con el script `/sbin/ifup`. Para detener o probar una interfaz, se puede utilizar `ifdown` y `ifstatus`.

Si sólo dispone de una tarjeta de red integrada en el ordenador, basta con que configure las interfaces a través del nombre. Con `ifup eth0`, `ifstatus eth0` y `ifdown eth0` puede iniciar, probar y parar la interfaz de red `eth0`. Los datos de configuración que se utilizan se encuentran en `/etc/sysconfig/network/ifcfg-eth0`. `eth0` es aquí tanto el nombre de la interfaz como el nombre de la configuración de la red.

De forma alternativa, la configuración de la red también puede asignar la dirección de hardware (dirección MAC) de una tarjeta de red. Para ello se utiliza un archivo de configuración `ifcfg-<dirección de hardware sin los dos puntos>`. Se debe escribir las letras de la dirección de hardware en minúsculas, tal y como se muestra con `ip link` (`ifconfig` utiliza mayúsculas). Cuando `ifup` encuentra un archivo de configuración que se adecúa a la dirección de hardware, se pasará por alto un `ifcfg-eth0` que pueda estar disponible.

Con las tarjetas de red que soportan `hotplug` es un poco más complicado. Si no tiene este tipo de tarjeta, puede pasar a la sección [Archivos de configuración](#) en la página siguiente.

Puesto que con tarjetas de red que soportan `hotplug` la asignación del nombre de la interfaz es aleatoria, las configuraciones de este tipo de tarjetas no se encuentran bajo del nombre de la interfaz, sino bajo un denominador que describe

el tipo de hardware utilizado y el punto de anclaje mencionados en la descripción de hardware que viene a continuación. En este caso `ifup` debe ser utilizado con dos argumentos: la descripción exacta del hardware y el nombre actual de la interfaz. Finalmente, `ifup` proveerá la configuración que más se ajusta a la descripción del hardware.

Como ejemplo tenemos un portátil con dos conexiones PCMCIA y una tarjeta de red Ethernet PCMCIA. Además en este aparato hay una tarjeta de red integrada con el nombre de interfaz `eth0`. Cuando insertamos esta tarjeta en el lugar de conexión 0, la descripción del hardware es `eth-pcmcia-0`. Ahora `cardmgr` o el script de red de hotplug invocan a `ifup eth-pcmcia-0 eth1`. `ifup` busca si existe un archivo `ifcfg-eth-pcmcia-0` en `/etc/sysconfig/network/`. Si no lo hay, seguirá buscando en `ifcfg-eth-pcmcia`, `ifcfg-pcmcia-0`, `ifcfg-pcmcia`, `ifcfg-eth1` y `ifcfg-eth`. El primer archivo que encuentre será el que utilice para la configuración. Cuando se deba definir una configuración de red válida para todas las tarjetas de red PCMCIA (en todos los puntos de conexión), esta se deberá llamar `ifcfg-pcmcia`. Esta servirá entonces tanto para `eth-pcmcia-0` como para una tarjeta Tokenring en el punto de conexión `1tr-pcmcia-1`.

También aquí tiene preferencia una configuración en función de la dirección de hardware, lo cual no hemos mencionado en el ejemplo por cuestiones de claridad.

YQST da un rodeo cuando se trata de configurar tarjetas de red que soporten hotplug. Allí se numeran las configuraciones para tales tarjetas. Por eso YQST siempre escribe las configuraciones para una tarjeta PCMCIA según `ifcfg-eth-pcmcia-<númeroactual>`. Para que a pesar de todo esta configuración sea válida para todos los puntos de conexión, se introduce un enlace `ifcfg-eth-pcmcia` en este archivo. Téngalo en cuenta si configura con YQST sólo parcialmente.

Archivos de configuración

En resumen, este apartado explica la función de los archivos de configuración de red y expone sus formatos.

/etc/sysconfig/network/ifcfg-* En estos archivos se incluyen los datos específicos de una interfaz de red. Se les puede denominar según el nombre de la interfaz (`ifcfg-eth2`), según la dirección de hardware de una tarjeta de red (`ifcfg-000086386be3`) o según la descripción de hardware de una tarjeta (`ifcfg-usb`). Si se utilizan alias de red,

los archivos necesarios se denominan simplemente `ifcfg-eth2:1` o `ifcfg-usb:1`. El script `ifup` recibe, junto al nombre de la interfaz, una precisa descripción de hardware, tras lo que busca el archivo de configuración más adecuado para la configuración.

Los archivos contienen la dirección IP (`BOOTPROTO="static"`, `IPADDR="10.10.11.214"`) o la indicación de utilizar DHCP (`BOOTPROTO="dhcp"`). Puede que la dirección IP ya contenga la máscara de red (`IPADDR="10.10.11.214/16"`) o se puede introducir aparte (`NETMASK="255.255.0.0"`). La lista completa de variables está en página del manual de `ifup` (`man ifup`). Además se pueden utilizar todas las variables de los archivos `dhcp`, `wireless` y `config` en `ifcfg-*`, en caso de que se deba utilizar una configuración general para una determinada interfaz. Con las variables `POST_UP_SCRIPT` y `PRE_DOWN_SCRIPT` se pueden tocar scripts individuales después del arranque o antes de la parada de la interfaz.

/etc/sysconfig/network/config, dhcp, wireless El archivo `config` incluye configuraciones generales para el comportamiento de `ifup`, `ifdown` y `ifstatus`. Este archivo está completamente comentado; también hay comentarios en `dhcp` y `wireless`, en los que tiene lugar las configuraciones generales para DHCP y tarjetas de red inalámbrica. También se pueden utilizar todas las variables de estos archivos en `ifcfg-*`, donde naturalmente tienen preferencia.

/etc/resolv.conf

Al igual que el archivo `/etc/host.conf`, este también juega un papel en la resolución de nombres de ordenadores a través de la librería *resolver*.

En este archivo se indica el dominio al que pertenece el ordenador. (Palabra clave `search`) y la dirección del servidor de nombres (palabra clave `nameserver`), al que se debe dirigir. Se puede introducir más nombres de dominio. Al resolver nombres que no estén totalmente cualificados se intentará generar un nombre válido y cualificado añadiendo entradas únicas en `search`. Se puede dar a conocer otros servidores de nombres añadiendo más líneas que comiencen con `nameserver`. Se puede introducir comentarios con `'#'`.

En el archivo [27](#), se muestra un ejemplo para `/etc/resolv.conf`.

```
# Our domain
search cosmos.univ
#
# We use sol (192.168.0.1) as nameserver
nameserver 192.168.0.1
```

Fichero 27: /etc/resolv.conf

¡YaST escribe aquí los servidores de nombres indicados!

Algunos servicios, como pppd (wvdial), ipppd (isdn), dhcp (dhcpcd y dhclient), pcmcia y hotplug pueden modificar los archivos `/etc/resolv.conf` mediante el script `modify_resolvconf`.

Al modificar el archivo `/etc/resolv.conf` con este script, aquel contendrá un comentario que da información sobre los servicios que se han modificado, el lugar donde se encuentra el archivo original y cómo se puede detener las modificaciones automáticas.

Si `/etc/resolv.conf` es modificado más veces, se volverá a limpiar este cúmulo de modificaciones cuando se recojan en otro orden; lo cual puede ocurrir con isdn, pcmcia y hotplug.

Si un servicio no ha finalizado "limpiamente", se puede restaurar el estado original con ayuda del script `modify_resolvconf`. Al arrancar se probará si un `resolv.conf` se ha quedado modificado (p. ej. debido a un cuelgue del sistema); en ese caso se volverá a restaurar el `resolv.conf` original (sin modificar).

Por medio de `modify_resolvconf check`, YaST averigua si el `resolv.conf` fue modificado, tras lo cual avisa al usuario de que se han perdido sus cambios tras la restauración. En caso contrario, YaST no utiliza `modify_resolvconf`, lo que quiere decir que una modificación en el archivo `resolv.conf` mediante YaST equivale a una modificación manual. Ambas indican una modificación duradera mientras que las realizadas por los servicios mencionados sólo son pasajeras.

/etc/hosts

Este archivo (ver archivo 28) tiene una tabla de asignación entre nombres de ordenadores y direcciones IP. En esta tabla deben aparecer todos los ordenadores con los que se quiere establecer una conexión IP cuando no se usa un servidor de nombres. Cada ordenador ocupa una línea en la tabla que contiene el número IP, el nombre completo de la máquina y el nombre (abreviado), p. ej. `tierra`. La línea debe comenzar con la dirección IP y las demás indicaciones se separan con espacios o tabuladores. Los comentarios comienzan con `'#'`.

```
127.0.0.1 localhost
192.168.0.1 sol.cosmos.univ sol
192.168.0.20 tierra.cosmos.univ tierra
```

Fichero 28: /etc/hosts

/etc/networks

En este archivo se convierten los nombres de redes en direcciones de red. El formato se parece al del archivo `hosts` sólo que aquí los nombres de las redes aparecen por delante de sus direcciones IP (ver archivo [29](#)).

```
loopback      127.0.0.0
localnet      192.168.0.0
```

Fichero 29: /etc/networks

/etc/host.conf

La resolución de nombres, o sea, la traducción del nombre del ordenador o de la red mediante la librería *resolver*, se gestiona a través de este archivo. El cual sólo se utiliza para programas con enlaces a `libc4` o `libc5`; ¡para programas `glibc` actuales, véase las configuraciones en `etc/nsswitch.conf`! Un parámetro debe ocupar una sola línea y los comentarios comienzan con `#`. Los parámetros posibles se muestran en la tabla [13.8](#).

<code>order hosts, bind</code>	Determina el orden de llamada a los servicios de resolución de nombres. Los parámetros posibles, separados por espacios o comas, son : <i>hosts</i> : Búsqueda en el archivo <code>/etc/hosts</code> <i>bind</i> : Llamada a un servidor de nombres <i>nis</i> : Mediante NIS
<code>multi on/off</code>	Determina si un ordenador dado de alta en <code>/etc/hosts</code> puede tener varias direcciones IP.
<code>nospoof on</code> <code>alert on/off</code>	Estos parámetros influyen sobre el " <i>spoofing</i> " del servidor de nombres, pero no tienen ninguna influencia adicional sobre la configuración de red.
<code>trim</code> <code><domainname></code>	El nombre de dominio que se indica aquí, se resta del nombre totalmente cualificado del ordenador que lo contiene (antes de asignar la dirección IP al nombre de ordenador). Se trata de una opción muy útil cuando el archivo <code>/etc/hosts</code> sólo contiene nombres de ordenadores locales (alias) y éstos deben ser reconocidos también cuando se añade el nombre del dominio.

Cuadro 13.8: *Parámetros de /etc/host.conf*

/etc/host.conf

Este archivo controla el funcionamiento de la librería de resolución, que convierte nombres de ordenadores en direcciones IP; este archivo solo se usa para programas que han sido enlazados con las librerías libc4 o libc5. ¡Para los programas actuales, enlazados con glibc, la configuración se encuentra en `/etc/nsswitch.conf`! Cada parámetro debe estar en una línea aparte. Los parámetros admitidos figuran en la tabla 13.8 en la página anterior; los comentarios comienzan con el símbolo '#’.

El archivo 30 muestra un ejemplo de `/etc/host.conf`.

```
# We have named running
order hosts bind
# Allow multiple addrs
multi on
```

Fichero 30: /etc/host.conf

/etc/nsswitch.conf

Con la versión 2.0 de la librería GNU de C comenzó el uso del "Name Service Switch" (NSS) (ver página del manual de `nsswitch.conf` (man 5 `nsswitch.conf`) y más explícito en *The GNU C Library Reference Manual*, capítulo "System Databases and Name Service Switch" – ver paquete `libcinfo`).

El archivo `/etc/nsswitch.conf` determina en cuál orden se solicitan determinadas informaciones. El archivo 31, muestra un ejemplo para `nsswitch.conf` en el cual las líneas de comentarios comienzan con '#’. Respecto a la "base de datos" `hosts`, el ejemplo siguiente indica que se envía una solicitud al servicio DNS (ver el apartado 13 en la página 339) después de consultar `/etc/hosts (files)`.

```
passwd:      compat
group:       compat

hosts:       files dns
networks:    files dns

services:    db files
protocols:   db files

netgroup:    files
automount:   files nis
```

Fichero 31: /etc/nsswitch.conf

Las “bases de datos” accesibles vía NSS se mencionan en la tabla 13.9. Para el futuro se espera también la disponibilidad de automount, bootparams, netmasks y publickey.

aliases	Mail-Alias, usado por sendmail(8); ver página del manual de aliases (man 5 aliases).
ethers	Direcciones de ethernet.
group	Usado por getgrent(3) para grupos de usuarios; ver página del manual de group (man 5 group).
hosts	Para nombres de host y direcciones IP, los usan funciones como gethostbyname(3) o parecidas.
netgroup	Lista de hosts y de usuarios válida en la red para administrar los derechos de acceso; ver página del manual de netgroup (man 5 netgroup).
networks	Nombres y direcciones de redes, lo usa getnetent(3).
passwd	Contraseñas de usuarios, que usa getpwent(3); ver página del manual de passwd (man 5 passwd).
protocols	Protocolos de red; información usada por getprotoent(3); ver página del manual de protocols (man 5 protocols).
rpc	Nombres y direcciones del tipo “Remote Procedure Call”; lo usan getrpcbyname(3) y otras funciones parecidas.
services	Servicios de red; lo usa getservent(3).
shadow	Las contraseñas “Shadow” de los usuarios, usado por getsppnam(3); ver página del manual de shadow (man 5 shadow).

Cuadro 13.9: Bases de datos accesibles a través de /etc/nsswitch.conf

Las opciones de configuración de las “bases de datos” NSS se encuentran en tabla 13.10 en la página siguiente.

files	acceso directo a los archivos, p. ej. a /etc/aliases.
db	acceso a través de una base de datos.

Cuadro 13.10: Continúa en la página siguiente...

<code>nis</code>	NIS, ver apartado 13 en la página 377.
<code>nisplus</code>	
<code>dns</code>	Parámetro adicional, solo aplicable para <code>hosts</code> y <code>networks</code> .
<code>compat</code>	Parámetro adicional para <code>passwd</code> , <code>shadow</code> y <code>group</code> .
<i>adicionalmente</i>	es posible conseguir diferentes resultados en caso de determinados eventos "Lookup"; hay detalles en página del manual de <code>nsswitch.conf</code> (<code>man 5 nsswitch.conf</code>).

Cuadro 13.10: Opciones de configuración de las "bases de datos" NSS

`/etc/nscd.conf`

Este es el archivo para configurar el `nscd` (ingl. *Name Service Cache Daemon*); ver página del manual de `nscd` (`man 8 nscd`) y página del manual de `nscd.conf` (`man 5 nscd.conf`). La información en cuestión es la que se encuentra en `passwd` y `groups`. `hosts` no es leído para no tener que reiniciar el daemon p.ej. cuando se cambia la resolución de nombres de dominio (DNS) modificando `/etc/resolv.conf`.

Cuando está activada la característica "caching" para `passwd`, normalmente pasan unos 15 segundos hasta que un usuario creado de nuevo se conozca en el sistema. Reiniciando `nscd` este tiempo de espera se puede reducir.

```
tierra:~ # rcnscd restart
```

`/etc/HOSTNAME`

Aquí se encuentra el nombre del ordenador, es decir, sólo el nombre del host sin el nombre de dominio. Hay distintos scripts que leen este archivo durante el arranque del ordenador. ¡No debe contener más que una sola línea con el nombre del ordenador!

Scripts de arranque (ingl. *Startup-Scripts*)

Aparte de los archivos de configuración mencionados, existen diferentes scripts (macros) que inician los programas de red cuando el ordenador arranca. Estos scripts se inician cuando el sistema entra en uno de los niveles de ejecución de multiusuario (ingl. *Multiuser-Runlevel*) (ver tabla 13.11 en la página siguiente).

<code>/etc/init.d/network</code>	Este script se encarga de la configuración del hardware y software de la red durante el arranque.
<code>/etc/init.d/inetd</code>	Inicia el <code>inetd</code> . Este se necesita p. ej. para acceder desde la red al ordenador en cuestión.
<code>/etc/init.d/portmap</code>	Inicia el "portmapper", que se necesita para usar servidores RPC como p. ej. un servidor NFS.
<code>/etc/init.d/nfsserver</code>	Inicia el servidor NFS.
<code>/etc/init.d/sendmail</code>	Controla el proceso de <code>sendmail</code> .
<code>/etc/init.d/ypserv</code>	Inicia el servidor NIS.
<code>/etc/init.d/ypbind</code>	Inicia el cliente NIS.

Cuadro 13.11: Algunos scripts de arranque de las utilidades de red

Routing en SuSE Linux

A partir de SuSE Linux 8.0 la tabla de "routing" es administrada en los archivos de configuración `/etc/sysconfig/network/routes` y `(etc/sysconfig/network/ifroute-*`.

El archivo `/etc/sysconfig/network/routes` define todas las rutas estáticas necesarias para las distintas tareas en un sistema: ruta hacia un ordenador, ruta hacia un ordenador a través de un gateway y ruta hacia una red..

Para todos las interfaces que tienen necesidad de "routing" individual existe la posibilidad de definir esto en un propio archivo por interfaz: `/etc/sysconfig/network/ifroute-*`. Cambie el símbolo `'*'` por el nombre del dispositivo. Un archivo podría contener líneas como estas:

```
DESTINATION      GATEWAY NETMASK  INTERFACE [ TYPE ] [ OPTIONS ]
DESTINATION      GATEWAY PREFIXLEN INTERFACE [ TYPE ] [ OPTIONS ]
DESTINATION/PREFIXLEN GATEWAY -      INTERFACE [ TYPE ] [ OPTIONS ]
```

Si `GATEWAY`, `NETMASK`, `PREFIXLEN` o `INTERFACE` no están indicadas hay que rellenar el campo correspondiente con el símbolo `'-'`. Los campos `TYPE` y `OPTIONS` pueden quedarse vacíos.

- El destino de una ruta se encuentra en la primera columna en forma de la dirección IP de una red o un ordenador. Si hay *acceso* a un servidor de

nombres, se puede usar también el nombre totalmente cualificado de la red o del ordenador.

- La segunda columna contiene el gateway por defecto o un gateway a través del cual se puede acceder a otro ordenador o red.
- La tercera columna contiene la máscara de red para redes u ordenadores detrás de un gateway. Por ejemplo, para un ordenador por detrás de un gateway el valor de la máscara es 255 . 255 . 255 . 255.
- La última columna solo es importante para las redes locales del ordenador (Loopback, Ethernet, RDSI, PPP, ...); en ella se apunta el nombre del dispositivo.

DNS – Domain Name System

El servicio DNS (ingl. *Domain Name System*) se encarga de convertir nombres de dominio y nombres de ordenadores en direcciones IP; generalmente se habla de "resolver nombres". Por ejemplo al nombre de ordenador `tierra` se le asigna la dirección IP `192.168.0.20`. Antes de configurar un DNS propio consulte la información general sobre DNS en el apartado [13](#) en la página [319](#)

Los siguientes ejemplos de configuración se refieren a BIND 9, el estándar actual en SuSE Linux.

Iniciar el servidor de nombres BIND

El servidor de nombres BIND (*Berkeley Internet Name Domain*) ya está preconfigurado en SuSE Linux por que puede iniciarse directamente después de la instalación.

Una vez que la conexión a Internet funciona, basta con introducir `127.0.0.1` como servidor de nombres para `localhost` en `/etc/resolv.conf` para que la resolución de nombres funcione sin necesidad de conocer el DNS del proveedor. De esta forma, BIND utiliza los "root name servers" para la resolución de los nombres y el proceso es mucho más lento. Por lo general, siempre se debería indicar la dirección IP del DNS del proveedor en el apartado `forwarders` del archivo de configuración `/etc/named.conf` para conseguir una resolución de nombres eficaz y segura. Funcionando de este modo, el servidor de nombres actúa en modo "caching-only". Configurándolo con zonas, se convierte en un DNS real. En el directorio de la documentación hay un ejemplo sencillo para ello: `/usr/share/doc/packages/bind9/sample-config`. No se debería configurar ningún dominio oficial mientras éste no haya sido asignado por parte de la institución en cuestión – para ".es" la organización ES-NIC es la que se encarga de ello. Aunque se disponga de un dominio propio, tampoco se debería utilizar mientras el proveedor se encargue de administrarlo. En caso contrario BIND deja de reenviar (forward) consultas para ese dominio y (p. ej.) el servidor web que se encuentra en el centro de datos del proveedor deja de estar accesible.

Como superusuario se puede iniciar el servidor de nombres mediante el comando: `rcnamed start`

Si a la derecha de la pantalla se muestra "done" en color verde, significa que el daemon del servidor de nombres (nombrado `named`) se ha iniciado correctamente. Los programas `host` o `dig` permiten comprobar inmediatamente el

funcionamiento en la máquina local. Como servidor predeterminado ha de constar `localhost` con la dirección `127.0.0.1`. Si éste no fuera el caso, es posible que `/etc/resolv.conf` contenga un servidor de nombres equivocado o que este archivo sencillamente no exista.

Con el comando `host 127.0.0.1` se puede comprobar si todo va bien. Si aparece un mensaje de error lo mejor es utilizar el comando

```
rcnamed status
```

para ver si el daemon `named` realmente está en funcionamiento. En caso de error, es posible averiguar el origen del mismo mediante los mensajes en el archivo `/var/log/messages`.

Para utilizar el servidor de nombres del proveedor o cualquier otro que ya exista en la red local como "forwarder", se introduce éste u otro en la entrada `forwarders` del apartado `options`. Las direcciones IP utilizadas en el archivo [32](#) han sido escogidas al azar y deben modificarse en función de su sistema.

```
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;  
};
```

Fichero 32: Opciones de reenvío o forwarding en `named.conf`

Detrás de `options` se encuentran las entradas para las zonas. Al menos siempre deberían existir las entradas de `localhost`, `0.0.127.in-addr.arpa` y `"` de `type hint`. No es necesario modificar los archivos correspondientes, ya que funcionan tal y como están. Además es importante que exista un `' ; '` al final de todas las entradas y que los corchetes estén correctamente colocados. Al haber modificado el archivo de configuración `/etc/named.conf` o los archivos de zona, es preciso que BIND vuelva a leer estos archivos. Esto se realiza con el comando `rcnamed reload`. Otra posibilidad es la de reiniciar el servidor mediante `rcnamed restart`; el comando para detenerlo es `rcnamed stop`.

El archivo de configuración `/etc/named.conf`

La configuración de BIND se realiza por completo con el archivo `/etc/named.conf`. Los datos propios de la zona, que son los nombres de los ordenadores,

direcciones IP, etc. de los dominios administrados, se han de anotar en archivos adicionales dentro del directorio `/var/lib/named`; en el siguiente capítulo se amplía esta información.

A grandes rasgos, `/etc/named.conf` se estructura en dos secciones; la primera es `options` para la configuración general y la siguiente es la que contiene las entradas `zone` para los diferentes dominios. También es posible utilizar una sección `logging` o una con entradas del tipo `acl` (ingl. *Access Control List*). Las líneas comentadas comienzan con el símbolo `'#' o '//'`.

El archivo 33 representa un `/etc/named.conf` muy sencillo.

```
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";
};
```

Fichero 33: archivo `/etc/named.conf` muy sencillo

Las opciones más importantes del apartado `options`

`directory "/var/lib/named";` indica el directorio que contiene los archivos con los datos de zona.

`forwarders { 10.0.0.1; };` se utiliza para indicar uno o varios servidores de nombres (generalmente los del proveedor) para pasarles las consultas DNS que no se pueden resolver directamente.

- forward first;** hace que las consultas DNS se reenvíen antes de tratar de resolverlas mediante un root name server. En lugar de **forward first** también es posible poner **forward only** para que todas las consultas sean siempre reenviadas sin acceder nunca a los root- name servers. Esta es una opción razonable para una configuración con cortafuegos.
- listen-on port 53 { 127.0.0.1; 192.168.0.1; };** indica las interfaces de red y el puerto que debe utilizar BIND para atender a las peticiones DNS realizadas por los clientes. Es posible suprimir **port 53**, ya que éste es el puerto estándar. Al suprimir esta entrada completamente, BIND atiende en todas las interfaces de red.
- listen-on-v6 port 53 { any; };** indica a BIND el puerto en el que ha de esperar las consultas de los clientes que utilizan IPv6. Además de **any** sólo se admite **none**, ya que el servidor siempre atiende a la dirección comodín de IPv6.
- query-source address * port 53;** Esta entrada puede resultar útil si un cortafuegos bloquea las consultas DNS externas, ya que BIND deja de utilizar los puertos altos (> 1024) y realiza entonces las consultas hacia fuera desde el puerto 53.
- query-source-v6 address * port 53;** Esta entrada debe utilizarse para las consultas realizadas a través de IPv6.
- allow-query { 127.0.0.1; 192.168.1/24; };** determina desde qué redes está permitido hacer consultas DNS. /24 es una abreviatura de la máscara de red, en este caso 255.255.255.0.
- allow-transfer { ! *; };** determina qué ordenadores pueden solicitar transferencias de zonas. ! * prohíbe totalmente la transferencia. Suprimiendo esta entrada, cualquier ordenador puede solicitar las transferencias de zona.
- statistics-interval 0;** Sin esta entrada, BIND crea cada hora varias líneas con datos estadísticos en `/var/log/messages`. Indicando 0, los mensajes se suprimen. El tiempo se expresa en minutos.
- cleaning-interval 720;** Esta opción indica el intervalo de limpieza de la cache de BIND. Cada vez que se realiza esta acción se crea una entrada en `/var/log/messages`. El tiempo se indica en minutos y el valor predeterminado es de 60 minutos.
- interface-interval 0;** BIND busca continuamente interfaces de red nuevas o canceladas Esta opción se suprime introduciendo el valor 0. De este modo, BIND sólo atiende las interfaces que existían en el momento del inicio. Es posible indicar un intervalo en minutos; el valor predeterminado es 60 minutos.

notify no; significa que el cambio de los datos de zona o cuándo se reinicia el servidor de nombres no se notifica a ningún otro servidor de nombres.

El apartado de configuración Logging

Hay muchas posibilidades de protocolar eventos con BIND. Normalmente la configuración predeterminada es suficiente. El archivo 34 muestra la forma más sencilla de una configuración que suprime el "Logging" totalmente:

```
logging {  
    category default { null; };  
};
```

Fichero 34: Logging suprimido

Estructura de las entradas de zona

Después de `zone` se indica el nombre de dominio a administrar (en este caso `mi-dominio.es`) seguido de `in` y un bloque de opciones entre corchetes; véase el archivo 35

```
zone "mi-dominio.es" in {  
    type master;  
    file "mi-dominio.zone";  
    notify no;  
};
```

Fichero 35: Configuración de mi-dominio.es

Para definir una "Slave-Zone" sólo hace falta cambiar `type` en `slave` e indicar un servidor de nombres que administra esta zona como `master` (igualmente puede ser un "slave"); véase el archivo 36.

```
zone "otro-dominio.es" in {  
    type slave;  
    file "slave/otro-dominio.zone";  
    masters { 10.0.0.1; };  
};
```

Fichero 36: Configuración para otro-dominio.es

Las opciones de zona:

type master; `master` significa que esta zona se administra en este servidor de nombres. Es algo que requiere un archivo de zona muy bien configurado.

type slave; Esta zona se transfiere de otro servidor de nombres. Hay que usarlo junto con `masters`.

type hint; La zona `.` del tipo `hint` se utiliza para indicar los root name servers. Es una definición de zona que no se modifica.

file "mi-dominio.zone"; file "slave/otro-dominio.zone"; Esta entrada indica el archivo que contiene los datos de zona para el dominio. En caso de un `slave` no hace falta que el archivo exista, ya que se trae desde otro servidor de nombres. Para separar los archivos de esclavo y de maestro, se indica `slave` como directorio de los archivos `slave`.

masters { 10.0.0.1; }; Esta entrada sólo se requiere para zonas esclavo e indica desde qué servidor de nombres se debe transferir el archivo de zona.

allow-update { ! *; }; Esta opción regula el acceso de escritura desde el exterior a los datos de zona. Es una opción que abre la posibilidad a los clientes de crear su propia entrada en el DNS, lo que no es deseable por razones de seguridad. Sin esta entrada las actualizaciones de zona están prohibidas, cosa que no cambia nada en este ejemplo, ya que `! *` prohíbe igualmente todo.

Sintaxis de los archivos de zona

Existen dos tipos de archivos de zona; el primero sirve para asignar la dirección IP a un nombre de ordenador y el segundo proporciona el nombre del ordenador en función de una dirección IP. El símbolo del punto (‘.’) tiene un significado importante en los archivos de zona. A todos los nombres de ordenadores que se indican sin el punto por detrás, se les añade la zona.

Por eso es importante terminar con un ‘.’ los nombres de las máquinas que se hayan anotado con el dominio completo. La falta o la posición equivocada de un punto suele ser la causa de error más frecuente en la configuración de un servidor de nombres. El primer ejemplo forma el archivo de zona `solar.zone` que corresponde al dominio `solar.sis`; véase el archivo [37](#).

```
1. $TTL 2D
2. solar.sis.    IN SOA      gateway root.solar.sis. (
3.              2003072441 ; serial
```

```

4.          1D          ; refresh
5.          2H          ; retry
6.          1W          ; expiry
7.          2D )        ; minimum
8.
9.          IN NS       gateway
10.         IN MX       10 sol
11.
12. gateway IN A        192.168.0.1
13.         IN A        192.168.1.1
14. sol     IN A        192.168.0.2
15. luna    IN A        192.168.0.3
16. tierra  IN A        192.168.1.2
17. marte   IN A        192.168.1.3
18. www     IN CNAME    luna

```

Fichero 37: archivo /var/lib/named/solar.zone

Línea 1: \$TTL define el TTL estándar, que vale para todas las anotaciones en este archivo y es en este caso de 2 días (2D = 2 days). TTL "time to live" es el tiempo de vencimiento.

Línea 2: Aquí comienza la parte del SOA control record:

- En primer lugar figura el nombre del dominio a administrar `solar.sis`, terminado con un `'.'` para que no se añada otra vez el nombre de la zona. La alternativa es la de anotar el símbolo `'@'` para que se busque el nombre de la zona en `/etc/named.conf`.
- Por detrás de `IN SOA` se anota el nombre del servidor de nombres que actúa como master para esta zona. En este caso, el nombre `gateway` se amplía a `gateway.solar.sis` ya que no termina con un 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 le reemplaza por un `'.'` - en lugar de `root@solar.sis` se escribe entonces `root.solar.sis.` No se debe olvidar el punto al final para que no se añada la zona.
- Al final hay un `'('`, para incorporar las siguientes líneas hasta el `')'` con todo el SOA-Record.

Línea 3: El número de serie en la línea `serial` es un número al azar que debe aumentarse después de cada modificación del archivo. El cambio del

número informa a los servidores de nombres secundarios sobre la modificación. Es típico utilizar una cifra de diez dígitos formada por la fecha y un número de orden en la forma AAAAMMDDNN.

Línea 4: El intervalo de refresco en la línea `refresh` indica al servidor de nombres secundario cuándo debe comprobar nuevamente la zona. En este caso es un día (1D = 1 day).

Línea 5: El intervalo de reintento en la línea `retry` indica cuánto tiempo después el servidor de nombres secundario debe intentar conectar nuevamente con el primario. En este caso son 2 horas (2H = 2 hours).

Línea 6: El tiempo de expiración en la línea `expiry` indica el tiempo después del cual el servidor de nombres secundario debe descartar los datos dentro de la caché, cuando la conexión con el servidor primario haya dejado de funcionar. En este caso es una semana (1W = 1 week).

Línea 7: La última entrada en SOA es el `negative caching TTL` que indica cuánto tiempo pueden mantener los otros servidores en la caché las consultas DNS hechas que no se han podido resolver.

Línea 9: `IN NS` indica el servidor de nombres que se encarga de este dominio. En este caso se vuelve a convertir `gateway` en `gateway.solar.sis` porque no se terminó con el 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` de `/etc/named.conf` tiene el valor `yes`, se informará de todos los servidores de nombres aquí mencionados y de los cambios en los datos de zona.

Línea 10: El MX-Record indica el servidor de correo que recibe, procesa o traspasa los mensajes para el dominio `solar.sis`. En este ejemplo se trata del ordenador `sol.solar.sis`. La cifra por delante del nombre de ordenador es 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 falla, se utiliza el servidor con el siguiente valor más alto.

Líneas 12-17: Estos son los registros de direcciones ((ingl. *address records*)) en los que se asignan una o varias direcciones IP a una máquina. Todos los nombres se anotaron sin el punto '.' al final, de tal forma que a todos se les añade `solar.sis`. El ordenador con el nombre `gateway` tiene dos direcciones IP asignadas porque dispone de dos tarjetas de red. El valor `A` representa una dirección tradicional de ordenador; `A6` hace referencia a direcciones IPv6 y `AAAA` es el formato obsoleto para las direcciones IPv6.

Línea 18: Con el alias `www` también es posible `luna` (CNAME = *canonical name*).

Para la resolución inversa de direcciones IP (ingl. *reverse lookup*) se utiliza el pseudo-dominio `in-addr.arpa`. Éste se añade por detrás a la parte de red de la dirección IP escrita al revés. `192.168.1` se convierte así en `1.168.192.in-addr.arpa`; véase 38.

```

1. $TTL 2D
2. 1.168.192.in-addr.arpa. IN SOA gateway.solar.sis. root.solar.sis. (
3.                               2003072441      ; serial
4.                               1D              ; refresh
5.                               2H              ; retry
6.                               1W              ; expiry
7.                               2D )           ; minimum
8.
9.                               IN NS          gateway.solar.sis.
10.
11. 1                               IN PTR       gateway.solar.sis.
12. 2                               IN PTR       tierra.solar.sis.
13. 3                               IN PTR       marte.solar.sis.
```

Fichero 38: Resolución de nombres inversa

Línea 1: `$TTL` define el TTL estándar que sirve en este caso para todas las configuraciones.

Línea 2: La resolución inversa “reverse lookup” se debe realizar para la red `192.168.1.0`. En este caso, la zona se denomina `1.168.192.in-addr.arpa` y este sufijo no se debe añadir a los nombres de las máquinas. Por eso, todos los nombres terminan con un punto. Para el resto se aplica lo mismo tal y como se explicó en el ejemplo anterior de `solar.sis`.

Línea 3-7: Véase el ejemplo anterior de `solar.sis`.

Línea 9: Esta línea indica también el servidor de nombres que se responsabiliza de la zona, pero en este caso se anota completamente con el `'.'` como terminación.

Líneas 11-13: Aquí se encuentran los registros de los punteros que apunten de una dirección IP a un nombre. Al comienzo de la línea sólo se encuentra la última cifra de la dirección IP sin el punto `'.'` como terminación. Añadiéndole la zona y quitando mentalmente la parte `.in-addr.arpa`, se obtiene la dirección IP completa en orden inverso.

Las transferencias de zonas entre las distintas versiones de BIND no deberían representar ningún problema.

Transacciones seguras

Las transacciones seguras pueden realizarse con ayuda de las "Transaction Signatures" (TSIG). Para ello se utilizan las claves de transacción (ingl. *transaction keys*) y las firmas de transacción (ingl. *transaction signatures*), cuya creación y uso se describen en las líneas siguientes.

Las transacciones seguras son necesarias para la comunicación entre servidores y para actualizar los datos de zonas dinámicamente. En este contexto, un control de los permisos basado en claves ofrece mucha más protección que un control basado en direcciones IP.

Para crear una clave de transacción puede utilizar el siguiente comando (obtendrá más información con página del manual de `dnssec-keygen` (`man dnssec-keygen`)):

```
dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2.
```

Al ejecutar este comando, se crean por ejemplo los archivos:

```
Khost1-host2.+157+34265.private  
Khost1-host2.+157+34265.key
```

La clave está incluida en ambos archivos (ej. `ejIkuCyyGJwwuN3xAteKgg==`). Para lograr una comunicación segura entre `host1` y `host2`, `Khost1-host2.+157+34265.key` ha de transmitirse de forma segura (p. ej. con `scp`) al ordenador remoto y allí ser introducida en `/etc/named.conf`.

```
key host1-host2. {  
    algorithm hmac-md5;  
    secret "ejIkuCyyGJwwuN3xAteKgg=";  
};
```

Aviso

Asegúrese de que los permisos de acceso a `/etc/named.conf` estén restringidos. El valor estándar es `0640` para `root` y el grupo `named`. De manera alternativa, también es posible guardar la clave en un archivo protegido propio y luego incluir este archivo.

Aviso

Para que en el servidor `host1` se utilice la clave para el `host2` con la dirección de ejemplo `192.168.2.3`, ha de realizarse la siguiente entrada en el `/etc/named.conf` del servidor:


```
server 192.168.2.3 {  
    keys { host1-host2. ; }  
};
```

En los archivos de configuración de `host2` deben también introducirse las entradas correspondientes.

Además de las ACLs basadas en direcciones IP y zonas de direcciones, también es necesario añadir claves TSIG para poder llevar a cabo transacciones seguras. Un posible ejemplo sería el siguiente:

```
allow-update { key host1-host2. ; };
```

Puede obtener más información en el manual de administración de BIND en el apartado `update-policy`.

Actualización dinámica de los datos de zonas

Actualización dinámica (ingl. *dynamic update*) es el término aplicado a las acciones de añadir, modificar o borrar entradas en los archivos de zona de un `master`. Este mecanismo se describe en RFC 2136.

En función de la zona, las actualizaciones dinámicas se configuran con las opciones `allow-update` o `update-policy` en las entradas de zona. Las zonas que se actualicen dinámicamente no deberían editarse de forma manual.

Las entradas que han de actualizarse son transmitidas al servidor con `nsupdate`. Puede consultar la estructura exacta en página del manual de `nsupdate` (man 8 `nsupdate`). Por motivos de seguridad, la actualización debería realizarse a través de transacciones seguras TSIG (sección 13 en la página anterior).

DNSSEC

DNSSEC (ingl. *DNS Security*) se describe en RFC 2535 y las herramientas disponibles para utilizar DNSSEC se encuentran recogidas en el manual de BIND.

Una zona segura debe disponer de una o varias claves de zona que, al igual que las claves de ordenador, son creadas con el comando `dnssec-keygen`. Para la codificación se toma actualmente DSA.

Las claves públicas (ingl. *public keys*) han de integrarse en los archivos de zonas con `$INCLUDE`.

Todas las claves se agrupan en un conjunto por medio del comando `dnssec-makekeyset`. Este conjunto se transmite a continuación de forma segura a la zona superior (ingl. *parent zone*) para ser firmado con `dnssec-signkey`. Los archivos generados durante la firma deben emplearse para firmar zonas con `dnssec-signzone` y los nuevos archivos generados deben ser a su vez integrados en `/etc/named.conf` para cada zona respectiva.

Información adicional

Entre las fuentes de información adicionales cabe destacar el manual de administración en inglés *BIND Administrator Reference Manual*, que está disponible en el sistema en `/usr/share/doc/packages/bind9/`. También se recomienda consultar los RFCs allí mencionados y las páginas del manual incluidas en BIND 9.

El servicio de directorio LDAP

En entornos de trabajo en red es de vital importancia el poder acceder de forma rápida y estructurada a la información que se necesita. Los datos desorganizados no sólo influyen negativamente en el uso de Internet, sino también pueden dificultar los procesos de búsqueda en la intranet de la empresa: ¿cuál es la extensión telefónica del Sr. X del departamento Y? ¿Y su dirección de correo electrónico?

Los servicios de directorio son la respuesta a este problema. De manera semejante a las páginas amarillas (ingl. *Yellow Pages*) en la vida ordinaria, dichos servicios contienen toda la información necesaria de forma estructurada y accesible.

En el caso ideal, un servidor central guarda los datos en un directorio y los distribuye a los clientes de la red a través de un protocolo determinado. Los datos han de estar estructurados de tal forma que un máximo número de aplicaciones pueda acceder a ellos. De este modo no es necesario que cada aplicación de calendario o cliente de correo electrónico disponga de una base de datos propia, sino basta con que puedan recurrir al depósito central, lo que reduce considerablemente el esfuerzo de administración de la información. El uso de un protocolo estandarizado y abierto como LDAP garantiza que el mayor número posible de aplicaciones de clientes tenga acceso a esta información.

En este contexto pues, un directorio es una especie de base de datos optimizada para poder ser examinada y leída muy fácil y rápidamente:

- Para permitir un alto número de accesos de lectura (simultáneos), los permisos de escritura están limitados a unas pocas actualizaciones por parte del administrador. Las bases de datos tradicionales están optimizadas para recoger en poco tiempo el mayor volumen de datos posible.
- Debido a que los permisos de escritura sólo pueden ejercerse de forma muy limitada, el servicio de directorio administra información *estática* que cambia rara vez. En contraposición, los datos en una base de datos convencional se modifican con mucha frecuencia (se trata de información *dinámica*). Por poner un ejemplo, los números de teléfono de un directorio de empleados están sujetos a muchos menos cambios que las cifras manejadas por el departamento de contabilidad.
- En la gestión de datos estáticos, los registros de datos se actualizan con muy poca frecuencia. En cambio, cuando se trabaja con datos dinámicos, especialmente en el terreno de cuentas bancarias y datos de contabilidad, la coherencia de los datos es primordial. Si una cantidad ha de restarse

de un sitio para ser añadida a otro, ambas operaciones han de ejecutarse simultáneamente en una "transacción" para garantizar la concordancia del conjunto de los datos. Las bases de datos soportan estas transacciones, mientras que los directorios no lo hacen. En estos últimos, la falta de concordancia de los datos resulta aceptable durante breves periodos de tiempo.

El diseño de un servicio de directorio como LDAP no está concebido para soportar complejos mecanismos de actualización o consulta. Todas las aplicaciones que accedan a este servicio han de poder hacerlo de la forma más fácil y rápida posible.

Han existido y existen numerosos servicios de directorio, no sólo en el mundo Unix, sino también, por ejemplo, Novells NDS, Microsofts ADS, Banyans Street Talk y el estándar OSI X.500.

Originalmente, LDAP fue planeado como una variante más simple de DAP (ingl. *Directory Access Protocol*) desarrollado para acceder a X.500. El estándar X.500 reglamenta la organización jerárquica de entradas de directorio.

LDAP no incorpora algunas de las funciones de DAP y puede ser utilizado en múltiples plataformas y, sobre todo, con un bajo consumo de recursos, sin renunciar a la jerarquía de entradas definida en X.500. Gracias al uso de TCP/IP es mucho más fácil implementar interfaces entre la aplicación y el servicio LDAP.

Entre tanto, LDAP ha seguido desarrollándose y se utiliza cada vez con más frecuencia como solución autónoma sin soporte X.500. Con LDAPv3 (la versión de protocolo disponible en su sistema con el paquete `openldap2` instalado), LDAP soporta remisiones o *referrals* que permiten implementar bases de datos distribuidas. Otra de las novedades consiste en la utilización de SASL ((ingl. *Simple Authentication and Security Layer*)) como capa de autenticación y protección.

LDAP no sólo puede aplicarse para consultar datos de servidores X.500 como era su propósito original: `slapd` es un servidor de código abierto u Open Source que permite guardar la información de un objeto en una base de datos local. Este servidor se complementa con `slurpd`, el cual se encarga de replicar varios servidores LDAP.

El paquete `openldap2` está formado fundamentalmente por dos programas.

slapd Un servidor LDAPv3 autónomo que gestiona la información de objetos en una base de datos basada en BerkeleyDB.

slurpd Este programa permite replicar los cambios realizados en los datos del servidor LDAP local en otros servidores LDAP instalados en la red.

Herramientas adicionales para el mantenimiento del sistema `slapcat`,
`slapadd`, `slapindex`

LDAP contra NIS

Tradicionalmente, los administradores de sistemas Unix utilizan el servicio NIS para la resolución de nombres y distribución de datos en la red. Los datos de configuración procedentes de los archivos `/etc` y los directorios `group`, `hosts`, `mail`, `netgroup`, `networks`, `passwd`, `printcap`, `protocols`, `rpc` y `services` son distribuidos entre los clientes de la red desde un servidor central. Como simples archivos de texto, estos archivos pueden mantenerse sin grandes dificultades. No obstante, la administración de cantidades mayores de datos resulta bastante más complicada debido a la falta de estructura. NIS está dirigido únicamente a plataformas Unix, lo que hace imposible su uso para la administración central de datos en redes heterogéneas.

Al contrario que NIS, el campo de aplicación del servicio LDAP no está limitado a redes sólo Unix. Los servidores Windows (2000 y superiores) soportan LDAP como servicio de directorio. Novell también ofrece un servicio LDAP. Además, sus funciones no se limitan a las mencionadas en líneas superiores.

El principio de LDAP puede aplicarse a cualquier estructura de datos que deba administrarse de forma centralizada. Entre los ejemplos de aplicación cabe destacar:

- Uso en sustitución de un servidor NIS
- Enrutamiento de correo (`postfix`, `sendmail`)
- Libreta de direcciones para clientes de correo como Mozilla, Evolution, Outlook, ...
- Administración de descripciones de zonas para un servidor de nombres BIND9

Esta enumeración podría prolongarse indefinidamente ya que LDAP, al contrario que NIS, es expandible. Su estructura de los datos claramente definida ayuda a la hora de administrar grandes cantidades de datos, ya que puede examinarse más fácilmente.

Estructura de un árbol de directorios LDAP

El directorio LDAP tiene una estructura en forma de árbol. Cada entrada (denominada objeto) del directorio ocupa una posición determinada dentro de esa jerarquía (denominada DIT o *Directory Information Tree*). La ruta completa a una entrada la identifica de modo inequívoco y se conoce como DN o *Distinguished Name*. Cada uno de los nodos en la ruta a dicha entrada se llaman RDN o *Relative Distinguished Name*. Por lo general, existen dos tipos de objetos:

Contenedor Este tipo de objeto puede contener a su vez otros objetos. Algunos ejemplos de estos elementos son `root` (elemento raíz del árbol de directorios que no existe en realidad), `c` (ingl. *country*), `ou` (ingl. *OrganizationalUnit*), y `dc` (ingl. *domainComponent*). Este modelo es equiparable a los directorios (carpetas) en el sistema de archivos.

Hoja Este tipo de objeto se encuentra al final de una rama y carece de objetos subordinados. Algunos ejemplos son `Person`/`InetOrgPerson` o `groupofNames`.

En la cúspide de la jerarquía del directorio se encuentra el elemento raíz `Root`. A este elemento le puede seguir en un nivel inferior `c` (ingl. *country*), `dc` (ingl. *domainComponent*) o `o` (ingl. *organization*).

El siguiente ejemplo ilustra mejor las relaciones jerárquicas dentro de un árbol de directorios LDAP (ver Figura 13.4).

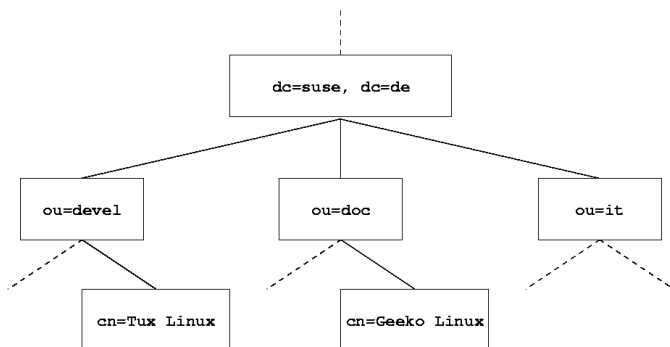


Figura 13.4: Estructura de un directorio LDAP

La figura representa un DIT ficticio con entradas ((ingl. *entries*)) en tres niveles. Cada entrada se corresponde con una casilla en la figura. En este caso, el nombre válido completo (DN o *Distinguished Name*) del empleado ficticio de Geeko

Linux es `cn=Geeko Linux, ou=doc, dc=suse, dc=de`. Este nombre se forma al añadir el RDN al DN de la entrada precedente `cn=Geeko Linux`.

La definición global de qué tipo de objetos han de guardarse en el DIT se realiza mediante un *esquema*. El tipo de objeto se determina mediante la *clase de objeto*. La clase de objeto especifica qué atributos *deben* o *pueden* ser asignados a un objeto determinado. Por lo tanto, un esquema debe contener definiciones de todas las clases de objetos y atributos que van a utilizarse en el escenario de aplicación. Existen algunos esquemas de uso extendido (véase RFC 2252 y 2256). No obstante, si el entorno en el que va a utilizarse el servidor LDAP lo requiere, también pueden crearse nuevos esquemas en función del usuario o pueden combinarse varios esquemas entre sí.

La tabla 13.12 ofrece un resumen de las clases de objetos utilizadas en el ejemplo de `core.schema` e `inetorgperson.schema` junto con los atributos obligatorios y los valores adecuados de atributo.

Clase de objeto	Significado	Entrada de ejemplo	Atributo obligatorio
<code>dcObject</code>	<i>domainComponent</i> (partes del nombre del dominio)	<code>suse</code>	<code>dc</code>
<code>organizationalUnit</code>	<i>organizationalUnit</i> (unidad organizativa)	<code>doc</code>	<code>ou</code>
<code>inetOrgPerson</code>	<i>inetOrgPerson</i> (datos sobre personal para Internet/intranet)	<code>Geeko Linux</code>	<code>sn</code> y <code>cn</code>

Cuadro 13.12: Clases de objetos y atributos de uso extendido

En la salida 15 puede ver un extracto de una instrucción de esquema con aclaraciones que le ayudarán a entender la sintaxis de nuevos esquemas.

```
...
#1 attributetype ( 2.5.4.11 NAME ( 'ou' 'organizationalUnitName' )
#2     DESC 'RFC2256: organizational unit this object belongs to'
#3     SUP name )

...
#4 objectclass ( 2.5.6.5 NAME 'organizationalUnit'
#5     DESC 'RFC2256: an organizational unit'
```

```

#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 )
...

```

***Mensaje en pantalla 15:** Extracto de `schema.core`
(Numeración de líneas para facilitar la comprensión)*

Como ejemplo se ha tomado el tipo de atributo `organizationalUnitName` y la clase de objeto correspondiente `organizationalUnit`. En la línea 1 aparece el nombre del atributo, su número de identificación de objeto (OID o *Object Identifier*) (numérico) y la abreviatura del atributo. En la línea 2, `DESC` introduce una breve descripción del atributo que incluye el RFC del que procede la definición. `SUP` en la línea 3 hace referencia a un tipo de atributo superior al que pertenece este atributo.

La definición de la clase de objeto `organizationalUnit` comienza en la línea 4 con un OID y el nombre de la clase de objeto, al igual que en la definición de atributo. La línea 5 contiene una breve descripción de la clase de objeto. La entrada `SUP top` en la línea 6 indica que esta clase de objeto no está subordinada a ninguna otra clase de objeto. La línea 7, que empieza por `MUST`, enumera todos los tipos de atributo que *deben* ser utilizados obligatoriamente en un objeto del tipo `organizationalUnit`. A continuación de `MAY` en la línea 8 se incluyen todos los tipos de atributos que *pueden* ser utilizados en conexión con esta clase de objeto.

La documentación del programa OpenLDAP, disponible en el sistema en `/usr/share/doc/packages/openldap2/admin-guide/index.html`, constituye una excelente introducción para la utilización de esquemas.

Configuración de servidor con `slapd.conf`

Su sistema instalado contiene un archivo de configuración completo para el servidor LDAP en `/etc/openldap/slapd.conf`. A continuación se explicarán brevemente cada una de las entradas y las modificaciones necesarias. Tenga en cuenta que las entradas precedidas del signo `"#"` se encuentran inactivas. Para activar dichas entradas basta con borrar el signo de comentario.

Instrucciones globales en slapd.conf

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/inetorgperson.schema
```

Mensaje en pantalla 16: slapd.conf: Instrucción Include para esquemas

Con esta primera instrucción en `slapd.conf` se define el esquema utilizado para organizar el directorio LDAP (ver salida 16). La entrada `core.schema` se requiere obligatoriamente. Si necesita esquemas adicionales, introdúzcalos detrás de esta instrucción (como ejemplo se ha añadido aquí `inetorgperson.schema`). Puede encontrar otros esquemas disponibles en el directorio `/etc/openldap/schema/`. Si NIS va a ser sustituido por un servicio LDAP, integre aquí los esquemas `cosine.schema` y `rfc2307bis.schema`. Puede obtener información adicional sobre este tema en la documentación incluida en OpenLDAP.

```
pidfile /var/run/slapd.pid
argsfile /var/run/slapd.args
```

Mensaje en pantalla 17: slapd.conf: pidfile y argsfile

Estos dos archivos contienen el número de identificación de proceso (PID o (ingl. *process id*)) y algunos argumentos con los que se iniciará el proceso `slapd`. En esta sección no es necesario realizar ningún cambio.

```
%
%

#
# 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!
```

Mensaje en pantalla 18: slapd.conf: Controles de acceso

La salida 18 en la página anterior es el fragmento de `slapd.conf` que regula los controles de acceso al directorio LDAP en el servidor. Las opciones definidas en esta sección global de `slapd.conf` tienen validez mientras no se especifiquen otras reglas de acceso en la sección específica de las bases de datos que sobreescriban a éstas. Conforme a las reglas aquí definidas, todos los usuarios tienen permiso de lectura para el directorio pero sólo el administrador (`rootdn`) puede escribir en el mismo. Debido a que la regulación de los permisos de acceso en LDAP es un tema muy complejo, incluimos a continuación unas reglas generales que le ayudarán a comprender este proceso:

- La sintaxis de todas las reglas de acceso es la siguiente:

```
access to <what> by <who> <access>
```

- *<what>* representa al objeto o atributo para el que quiere definir el acceso. Puede proteger de forma explícita diversas ramas del directorio o bien cubrir zonas enteras del árbol de directorios por medio de expresiones regulares. `slapd` evalúa todas las reglas en el orden en el que aparecen en el archivo de configuración. Por lo tanto, anteponga siempre las reglas más restrictivas a las más generales. `slapd` analiza la primera regla aplicable que encuentra e ignora el resto.
- *<who>* define quién tiene acceso a los sectores definidos en *<what>*. El uso de expresiones regulares le ahorrará aquí también mucho trabajo. Como en el caso anterior, `slapd` interrumpe el proceso de análisis de *<who>* al encontrar la primera regla aplicable. Por lo tanto, las reglas específicas han de anteponerse de nuevo a las más generales. Pueden utilizarse las siguientes entradas (ver tabla 13.13 en la página siguiente):

Identificador	Significado
*	todos los usuarios sin excepción
anonymous	usuarios no autenticados ("anónimos")
users	usuarios autenticados
self	usuarios unidos al objeto destino
dn=<regex>	todos los usuarios a los que puede aplicarse esta expresión regular

Cuadro 13.13: Grupos de usuarios con acceso autorizado

- `<access>` especifica el tipo de acceso. Aquí se distingue entre las posibilidades que aparecen en la tabla 13.14:

Identificador	Significado
<code>none</code>	acceso prohibido
<code>auth</code>	para contactar con el servidor
<code>compare</code>	para accesos comparables a objetos
<code>search</code>	para utilizar filtros de búsqueda
<code>read</code>	permiso de lectura
<code>write</code>	permiso de escritura

Cuadro 13.14: Tipos de acceso

`slapd` compara los permisos solicitados por el cliente con los que han sido concedidos en `slapd.conf`. Si allí están autorizados derechos iguales o más amplios que los que solicita el cliente, éste obtiene autorización. Si por el contrario el cliente solicita más permisos que los concedidos en `slapd.conf`, el acceso será denegado.

La salida 19 contiene un ejemplo muy simple de un control de acceso sencillo que puede configurarse de la forma deseada utilizando expresiones regulares.

```
access to dn.regex="ou=( [^, ]+),dc=suse,dc=de"
by cn=administrator,ou=$1,dc=suse,dc=de write
by user read
by * none
```

Mensaje en pantalla 19: `slapd.conf`: Ejemplo de control de acceso

Según esta regla, sólo el administrador tiene permiso de escritura para todas las entradas `ou`, los usuarios autenticados disponen de permiso de lectura, y al resto se le ha denegado el acceso.

Truco

Definición de reglas Access

Si no es posible aplicar ninguna regla `access to` o instrucción `by <who>`, el permiso será denegado. Sólo se conceden aquellos permisos autorizados explícitamente. En caso de no existir ninguna regla, se aplica el siguiente principio: permiso de escritura para el administrador y permiso de lectura para todos los demás.

Truco

La documentación en línea del paquete instalado `openldap2` incluye información más detallada y una configuración de muestra de los permisos de acceso para LDAP.

Además de la administración de los permisos de acceso a través del archivo de configuración central (`slapd.conf`), existe también la posibilidad de utilizar informaciones de control de acceso o ACIs ((ingl. *Access Control Information*)). Las ACIs permiten almacenar la información de acceso a cada objeto en el mismo árbol LDAP. Debido a que este tipo de control de acceso está todavía muy poco extendido y su estado ha sido calificado por los desarrolladores como experimental, referimos aquí a la documentación del proyecto OpenLDAP en Internet: <http://www.openldap.org/faq/data/cache/758.html>.

Instrucciones para bases de datos en `slapd.conf`

```
database          ldbm
suffix            "dc=suse,dc=de"
rootdn            "cn=admin,dc=suse,dc=de"
# Cleartext passwords, especially for the rootdn, should
# be avoided. See slapdpasswd(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
```

Mensaje en pantalla 20: `slapd.conf`: Instrucciones para bases de datos

En la primera línea de esta sección (ver salida 20) se define el tipo de base de datos, LDBM en este caso. La entrada `suffix` de la segunda línea especifica la parte del árbol de directorios LDAP de la que se va a ocupar este servidor. En la línea inferior, `rootdn` determina quién dispone de derechos de administración

para este servidor. No es necesario que el usuario indicado en esta sección posea una entrada LDAP o que exista siquiera como usuario "normal". La contraseña de administrador se define con la instrucción `rootpw`. Aquí puede sustituir `secret` por el resumen criptográfico generado con `slappasswd`. La instrucción `directory` indica el directorio en el que están almacenados los directorios de la base de datos en el servidor. La última instrucción, `index objectClass eq`, hace que se cree un índice con las clases de objetos. Si lo desea, puede introducir otros atributos que en su caso particular se busquen con más frecuencia. Cuando se definen reglas `Access` propias para la base de datos y se colocan detrás, se aplicarán éstas en lugar de las reglas `Access` globales.

Iniciar y parar el servidor

Una vez que el servidor LDAP ha sido configurado y en el directorio LDAP se han llevado a cabo todas las entradas deseadas según el modelo descrito abajo (ver apartado [Administración de datos en el directorio LDAP](#) en esta página), puede iniciar el servidor LDAP como usuario `root` introduciendo el siguiente comando:

```
rcldap start
```

Para detener el servidor de forma manual ha de introducir el comando `rcldap stop` y para consultar el estado del servidor, `rcldap status`.

También es posible configurar el servidor para que se inicie y detenga automáticamente al encender y apagar al ordenador. Para ello puede utilizar el editor de niveles de ejecución de `YAST` (véase el apartado [El editor de niveles de ejecución de YaST](#) en la página 303) o bien crear directamente los enlaces correspondientes en los scripts de inicio y final por medio de `insserv` en la línea de comandos (ver apartado [Añadir scripts init](#) en la página 301).

Administración de datos en el directorio LDAP

OpenLDAP proporciona al administrador numerosos programas para gestionar los datos en el directorio LDAP. A continuación le presentamos los cuatro programas más importantes para añadir, eliminar, examinar y modificar los datos existentes.

Introducir datos en el directorio LDAP

Como condición previa para la introducción de nuevas entradas, la configuración del servidor LDAP en `/etc/openldap/slapd.conf` ha de ser correcta y apta para su aplicación, es decir, debe contener las instrucciones adecuadas para

suffix, directory, rootdn, rootpw e index. La introducción de entradas en OpenLDAP puede llevarse a cabo con el comando `ldapadd`. Por razones prácticas se recomienda añadir los objetos a la base de datos en forma de paquetes. Con este fin, LDAP contempla el formato LDIF ((ingl. *LDAP Data Interchange Format*)). Un archivo LDIF es un simple archivo de texto que puede estar formado por un número indeterminado de pares de atributo y valor. Puede consultar los objetos y atributos disponibles en los archivos de esquemas indicados en `slapd.conf`. El archivo LDIF utilizado para crear el armazón del ejemplo de la figura 13.4 en la página 354 podría presentar el siguiente aspecto (ver archivo 39):

```
# La organización SuSE
dn: dc=suse,dc=de
objectClass: dcObject
objectClass: organization
o: SuSE AG
dc: suse

# La unidad de organización Desarrollo (devel)
dn: ou=devel,dc=suse,dc=de
objectClass: organizationalUnit
ou: devel

# La unidad de organización Documentación (doc)
dn: ou=doc,dc=suse,dc=de
objectClass: organizationalUnit
ou: doc

# La unidad de organización Administración de Sistemas (it)
dn: ou=it,dc=suse,dc=de
objectClass: organizationalUnit
ou: it
```

Fichero 39: Ejemplo de archivo LDIF

Atención**Codificación de los archivos LDIF**

LDAP funciona con UTF-8 (Unicode), por lo que caracteres especiales como acentos, etc., han de introducirse con la codificación correcta. Utilice para ello editores que soporten UTF-8, como *Kate* o versiones actuales de *Emacs*). De lo contrario, deberá usar *recode* para convertir el texto a UTF-8.

Atención

Guarde el archivo como `<archivo>.ldif` y páselo al servidor con el siguiente comando:

```
ldapadd -x -D <dn del administrador> -W -f <archivo>.ldif
```

La primera opción `-x` indica que en este caso no se va a producir una autenticación a través de SASL. `-D` identifica al usuario que realiza esta operación. Introduzca aquí el DN válido del administrador tal y como ha sido configurado en `slapd.conf` (en nuestro ejemplo, `cn=admin,dc=suse,dc=de`). `-W` evita tener que introducir la contraseña en la línea de comandos (texto en claro) y activa una pregunta por separado de la contraseña. Dicha contraseña ha sido especificada previamente en `slapd.conf` en la entrada `rootpw`. `-f` pasa el archivo al servidor. A continuación se muestra la salida 21 de `ldapadd`:

```
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"
```

Mensaje en pantalla 21: ldapadd de ejemplo.ldif

Los datos de usuario de los empleados de cada uno de los departamentos pueden introducirse en archivos LDIF adicionales. Por medio del siguiente ejemplo `tux.ldif` (ver la salida 22), el empleado Tux es añadido al nuevo directorio LDAP:

```
# El empleado Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
objectClass: inetOrgPerson
```

```
cn: Tux Linux
givenName: Tux
mail: tux@suse.de
uid: tux
telephoneNumber: +34 123 4567-8
```

Mensaje en pantalla 22: Archivo LDIF para Tux

Un archivo LDIF puede contener un número ilimitado de objetos. Es posible pasar al servidor árboles de directorios completos de una vez o sólo partes de los mismos, como por ejemplo objetos sueltos. Si necesita modificar los datos con frecuencia, se recomienda el fraccionamiento en objetos individuales para evitar laboriosas búsquedas en archivos grandes del objeto que debe ser modificado.

Modificar datos en el directorio LDAP

Los registros de datos pueden modificarse con la herramienta `ldapmodify`. El método más fácil consiste en editar el archivo LDIF respectivo y pasar de nuevo el archivo modificado al servidor LDAP. Por ejemplo, para cambiar el número de teléfono del empleado Tux de +34 123 4567-8 a +34 123 4567-10, edite el archivo LDIF como se muestra en [23](#).

```
# El empleado Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
changetype: modify
replace: telephoneNumber
telephoneNumber: +34 123 4567-10
```

Mensaje en pantalla 23: Archivo LDIF tux.ldif modificado

Utilice el siguiente comando para importar el archivo modificado al directorio LDAP:

```
ldapmodify -x -D cn=admin,dc=suse,dc=de -W -f tux.ldif
```

Como alternativa, también puede introducir directamente en la línea de comandos los atributos que deben ser modificados con `ldapmodify`. En este caso proceda como se describe a continuación:

- Ejecute `ldapmodify` e introduzca su contraseña:

```
ldapmodify -x -D cn=admin,dc=suse,dc=de -W
Enter LDAP password:
```


- Introduzca los cambios siguiendo la estructura definida a continuación y el orden especificado:

```
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
changetype: modify
replace: telephoneNumber
telephoneNumber: +34 123 4567-10
```

Puede obtener información detallada sobre `ldapmodify` y su sintaxis en la página del manual correspondiente (`man ldapmodify`).

Buscar o leer datos del directorio LDAP

OpenLDAP ofrece `ldapsearch`, una herramienta de línea de comandos para examinar y leer datos en el directorio LDAP. La sintaxis de un comando de búsqueda sencillo sería la siguiente:

```
ldapsearch -x -b "dc=suse,dc=de" "(objectClass=*)"
```

La opción `-b` define la base de búsqueda, es decir, la sección del árbol donde va a efectuarse la búsqueda (en este caso, `dc=suse, dc=de`). Si desea realizar una búsqueda más depurada en subsecciones determinadas del directorio LDAP (por ejemplo sólo en el departamento `devel`), puede definir dicha sección en `ldapsearch` con la opción `-b`. La opción `-x` especifica la utilización de una autenticación sencilla. `(objectClass=*)` indica que desea leer todos los objetos incluidos en el directorio. Puede utilizar este comando tras la creación de un nuevo árbol de directorios para comprobar si todas las entradas han sido aceptadas correctamente y si el servidor responde en la forma deseada. Puede obtener información adicional sobre el uso de `ldapsearch` en su página del manual (`man ldapsearch`).

Borrar datos del directorio LDAP

Utilice el comando `ldapdelete` para borrar entradas del directorio LDAP. Su sintaxis es muy semejante a la de los comandos descritos en líneas superiores. Por ejemplo, para borrar la entrada completa de `Tux Linux`, introduzca el comando:

```
ldapdelete -x -D "cn=admin,dc=suse,dc=de" -W cn=Tux \
Linux,ou=devel,dc=suse,dc=de
```

Configuración de LDAP con YaST

Atención

Configuración del servidor LDAP

YaST le ayuda a la hora de organizar las entradas del directorio pero no a configurar el directorio LDAP en sí. Antes de que empiece a trabajar con el cliente LDAP de YaST, el servidor LDAP ha de estar configurado correctamente (integración de esquemas, ACLs adecuadas, proceso de inicio, etc.). Además de los esquemas típicos de NIS (`rfc2307bis.schema` y `cosine.schema`), es necesario añadir `yast2userconfig.schema` a la lista de esquemas. Asimismo, el servidor LDAP ha de disponer de al menos una entrada base bajo la que puedan ordenarse todas las entradas adicionales. Cree esta entrada como archivo `.ldif` como se ha descrito anteriormente con el comando `ldapadd`.

Atención

SuSE Linux le ofrece la oportunidad de utilizar LDAP en lugar de NIS para administrar los datos de grupos y usuarios. El módulo ‘Servicios de red’ → ‘Cliente LDAP’ de YaST permite configurar la autenticación de usuarios en la red. Aquí puede activar el uso de LDAP para administrar la información de usuario y definir entradas estándar que deberán ser consultadas al crear nuevos usuarios y grupos en los correspondientes módulos de YaST.

Procedimiento general

Para entender la función del módulo LDAP de YaST, es necesario conocer a grandes rasgos los procesos que se ejecutan en segundo plano en el ordenador cliente. Tras haber activado durante la instalación el uso de LDAP para la autenticación en red o iniciado el módulo de YaST, los paquetes `pam_ldap` y `nss_ldap` son instalados y los archivos de configuración correspondientes adaptados.

Con `pam_ldap` se utiliza el módulo PAM, el cual actúa como intermediario entre los procesos de registro al sistema y el directorio LDAP como fuente de datos para la autenticación. El módulo de software responsable, `pam_ldap.so`, es instalado y el archivo de configuración de PAM se modifica de forma correspondiente (ver salida [24](#)).

```
auth:      use_ldap nullok
account:   use_ldap
password:  use_ldap nullok
session:   none
```

Mensaje en pantalla 24: pam_unix2.conf adaptado para LDAP

Si desea configurar manualmente servicios adicionales para el uso de LDAP, el módulo PAM-LDAP ha de ser añadido al archivo de configuración PAM correspondiente a dicho servicio en `/etc/pam.d/`. Puede encontrar archivos de configuración ya adaptados para diversos servicios en `/usr/share/doc/packages/pam_ldap/pam.d/`. Copie los archivos respectivos en `/etc/pam.d/`.

Con `nss_ldap` adapta la resolución de nombres de `glibc` al uso de LDAP mediante el mecanismo `nsswitch`. Al instalar este paquete, se crea un nuevo archivo modificado `nsswitch.conf` en `/etc/`. Puede obtener más información sobre la función de `nsswitch.conf` en la sección [Archivos de configuración](#) en la página 330. Su archivo `nsswitch.conf` ha de contener las siguientes líneas para la administración y autenticación de usuarios por medio de LDAP (ver salida 25):

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

Mensaje en pantalla 25: Archivo nsswitch.conf adaptado

Estas líneas indican a la librería de resolución de `glibc` que evalúe en primer lugar los archivos locales guardados en `/etc` como fuente para los datos de usuarios y autenticación, y consulte de manera complementaria al servidor LDAP. Pruebe este mecanismo ejecutando el comando `getent passwd` para leer, por ejemplo, el contenido de la base de datos de usuario. En el resultado deberían mostrarse tanto los usuarios locales de su sistema como los usuarios creados en el servidor LDAP.

Módulos y plantillas: configuración con YaST

Una vez que YaST ha adaptado los archivos `nss_ldap` y `pam_ldap`, puede comenzar con el auténtico proceso de configuración en la primera máscara de YaST.

Atención

Aplicación del cliente de YaST

El cliente LDAP de YaST se emplea para adaptar los módulos de YaST a la administración de usuarios y grupos y ampliarlos en caso necesario. Asimismo tiene la posibilidad de definir plantillas con valores estándar para cada uno de los atributos con el fin de simplificar la recogida de datos. Los valores aquí prefijados son guardados como objetos LDAP en el directorio LDAP. Los datos de usuario se siguen recogiendo a través de las máscaras de los módulos de YaST y los datos recogidos se guardan como objetos en el directorio LDAP.

Atención

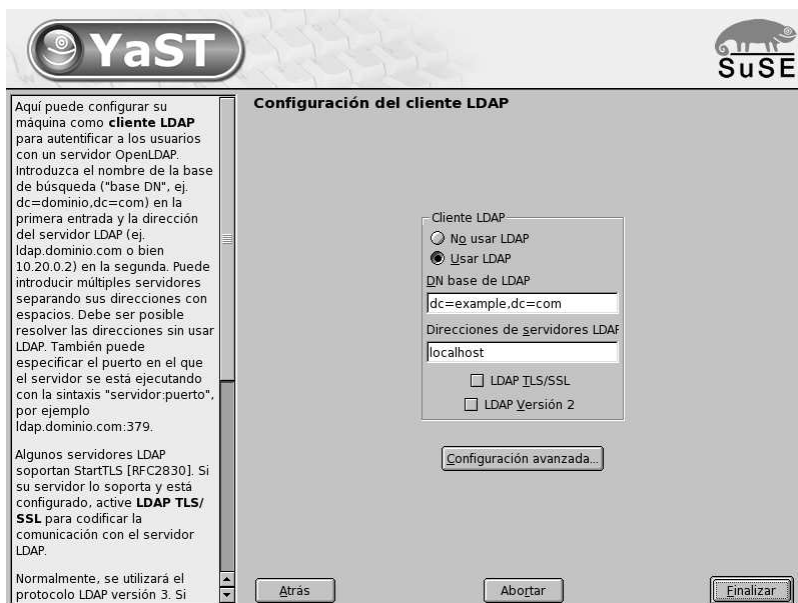


Figura 13.5: YaST: Configuración del cliente LDAP

En el primer diálogo, active la casilla para utilizar LDAP para la autenticación de usuarios e introduzca en 'DN base de LDAP' la base de búsqueda en el servidor donde están guardados todos los datos en el servidor LDAP. En el segundo apartado, 'Direcciones de servidores LDAP', ha de introducir la dirección del servidor LDAP. Si el servidor soporta StartTLS, active la casilla 'LDAP TLS/SSL' para posibilitar la comunicación cifrada entre el cliente y el servidor. Si desea

poder modificar datos de forma activa en el servidor como administrador, pulse el botón ‘Configuración avanzada’.



Figura 13.6: YaST: Configuración avanzada

Introduzca aquí los datos de accesos necesarios para poder modificar las opciones de configuración en el servidor LDAP. Estos datos son ‘Configuración DN base’, donde están guardados todos los objetos de la configuración, y ‘Bind DN’. El BIND DN es en este caso su DN de usuario.

Active la casilla ‘Servidor de archivos’ si el ordenador en el que ejecuta este módulo de YaST actúa como servidor de archivos en la red.

Pulse en ‘Configurar valores guardados en el servidor’ para editar las entradas del servidor LDAP. A continuación aparece un menú emergente en el que debe introducir su contraseña LDAP para autenticarse en el servidor. En función de las ACLs o ACIs del servidor, se le permitirá acceder a los módulos de configuración en éste.

Truco

Actualmente, YaST sólo soporta los módulos de administración de grupos y usuarios.

Truco



Figura 13.7: YaST: Configuración de módulos

El diálogo de la configuración de módulos le permite seleccionar y modificar módulos ya existentes, crear nuevos módulos o crear y editar plantillas ((*ingl. templates*)) para dichos módulos. Para cambiar un valor dentro de un módulo de configuración o cambiar el nombre de un módulo, seleccione el tipo de módulo en el cuadro de diálogo que se encuentra sobre el resumen de contenidos del módulo actual. En dicho resumen de contenidos aparece entonces una tabla con todos los atributos permitidos para este módulo y sus valores correspondientes. Además de los atributos ya definidos, la lista incluye los atributos permitidos para el esquema empleado aunque no se estén utilizando en ese momento. Si desea copiar un módulo, cambie simplemente **cn**. Para modificar valores de atributos, selecciónelos en el resumen de contenidos y pulse 'Editar'. A continuación se abre una ventana de diálogo en la que puede cambiar todas las opciones de configuración del atributo. Finalmente, confirme los cambios con 'OK'.

Si desea complementar un módulo ya existente con un nuevo módulo, pulse el botón 'Nuevo' sobre el resumen de contenidos. Después introduzca en el diálogo emergente la clase de objeto del nuevo módulo (*userConfiguration* o *groupConfiguration* en este caso) y el nombre del nuevo módulo. Ahora salga del diálogo con 'OK': el nuevo módulo será añadido a la lista de selección de los módulos disponibles. A partir de ahora, el módulo ya puede seleccionarse y

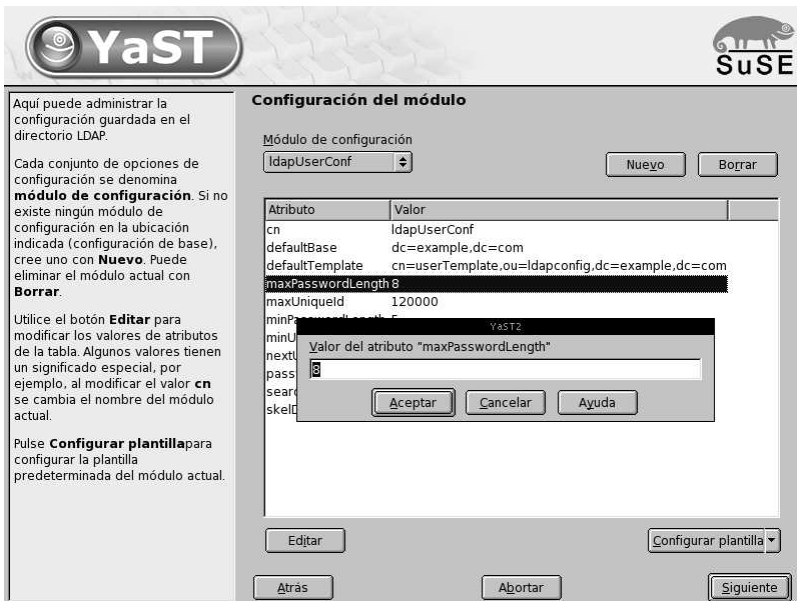


Figura 13.8: YaST: Edición de atributos en la configuración de módulos

deseleccionarse en el cuadro de diálogo. Para eliminar el módulo seleccionado actualmente, pulse el botón 'Borrar'.

Los módulos de YaST para la administración de grupos y usuarios unen plantillas con valores estándar adecuados siempre que éstos hayan sido definidos previamente con el cliente LDAP de YaST. Para adaptar una plantilla a sus requisitos, pulse el botón 'Configurar plantilla'. A continuación se muestra un menú desplegable con plantillas existentes que pueden ser editadas o bien una entrada vacía con la que también se accede a la máscara de edición de plantillas. Seleccione una entrada y defina las propiedades de la plantilla en la máscara siguiente 'Configuración de la plantilla de objeto'. Dicha máscara está dividida en dos ventanas con formato de tabla. La ventana superior contiene una lista de atributos generales de plantillas. Asigne valores a estos atributos en función de sus requisitos o deje algunos vacíos. Los atributos "vacíos" son borrados del servidor LDAP.

La segunda ventana ('Valores predeterminados para nuevos objetos') muestra todos los atributos del objeto LDAP correspondiente (configuración de grupos o usuarios en este caso) para los que define un valor estándar. También puede añadir nuevos atributos con sus respectivos valores estándar, editar atributos



Figura 13.9: YaST: Crear un módulo nuevo

y valores existentes o eliminar atributos completos. Al igual que los módulos, los atributos pueden copiarse modificando la entrada `cn` para crear una plantilla nueva. Para unir una plantilla con el módulo correspondiente, asigne como valor del atributo `defaultTemplate` del módulo el DN de la plantilla modificada tal y como se ha descrito arriba.

Truco

Puede crear un valor estándar para un atributo a partir de otros atributos mediante la utilización de variables en lugar de valores absolutos. Por ejemplo, a la hora de crear un usuario, `cn=%sn%givenName` se crea automáticamente de los valores de atributos de `sn` y `givenName`.

Truco

Una vez que todos los módulos y plantillas están configurados correctamente y listos para el uso, puede crear nuevos grupos y usuarios con YaST de la forma acostumbrada.



Figura 13.10: YaST: Configuración de una plantilla de objeto

Usuarios y grupos: configuración con YaST

Después de que la configuración de módulos y plantillas para la red se ha llevado a cabo, la recogida de datos para usuarios y grupos no difiere apenas del procedimiento normal sin utilizar LDAP. La siguiente descripción se ocupa únicamente de la administración de usuarios. La administración de grupos discurre de manera análoga.

Para acceder a la administración de usuarios en YaST ha de seleccionar 'Seguridad y usuarios' → 'Editar y crear usuarios'. Para crear un nuevo usuario, pulse el botón 'Añadir'. A continuación pasa a una máscara donde debe rellenar los datos de usuario más importantes tales como nombre, login y contraseña. Tras completar esta máscara, pulse en 'Detalles' para completar opciones más avanzadas de configuración como la pertenencia a grupos, la shell de login y el directorio local de usuario. Los valores predeterminados de los campos de entrada ya han sido configurados según el procedimiento descrito en el apartado *Módulos y plantillas: configuración con YaST* en la página 367. Si ya ha activado la utilización de LDAP, desde esta máscara pasa a otra donde se introducen los atributos específicos de LDAP (ver Figura 13.12 en la página 375). Seleccione uno tras otro los atributos cuyo valor desea modificar y pulse en 'Editar' para abrir los cam-



Figura 13.11: YaST: Administración de usuarios

pos de entrada correspondientes. Después pulse ‘Siguiente’ para abandonar la máscara y se encontrará de nuevo en la máscara de inicio de la administración de usuarios.

En la máscara de inicio de la administración de usuarios (ver Figura 13.11) se encuentra el botón ‘Opciones avanzadas’, que le permite aplicar filtros de búsqueda LDAP a los usuarios disponibles o configurar por primera vez el cliente LDAP de YaST a través de la opción ‘Configurar cliente LDAP’.

Información adicional

En este capítulo se han omitido de forma consciente temas de cierta complejidad como la configuración de SASL o de un servidor LDAP de replicación que comparte el trabajo con varios esclavos (“slaves”). Puede encontrar información detallada sobre ambos temas en *OpenLDAP 2.1 Administrator’s Guide* (ver enlace más abajo).

La página web del proyecto OpenLDAP contiene abundante documentación en inglés para usuarios de LDAP tanto novatos como expertos:

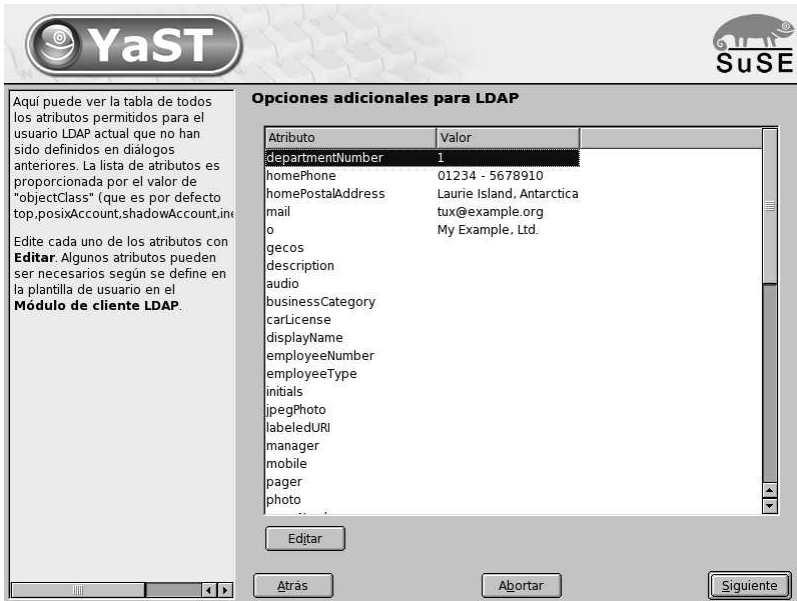


Figura 13.12: YaST: Opciones adicionales para LDAP

OpenLDAP Faq-O-Matic Una extensa colección de preguntas y respuestas en torno a la instalación, configuración y utilización de OpenLDAP.

<http://www.openldap.org/faq/data/cache/1.html>.

Quick Start Guide Breves instrucciones paso a paso para su primer servidor LDAP

<http://www.openldap.org/doc/admin21/quickstart.html>

o bien en su sistema instalado en /usr/share/doc/packages/openldap2/admin-guide/quickstart.html

OpenLDAP 2.1 Administrator's Guide Una detallada introducción a todos los aspectos importantes de la configuración de LDAP incluyendo codificación y control de acceso

<http://www.openldap.org/doc/admin21/> o bien en su sistema instalado en /usr/share/doc/packages/openldap2/admin-guide/index.html

Los siguientes libros rojos (redbooks) de IBM tratan también de LDAP:

Understanding LDAP Una introducción general muy amplia a los principios básicos de LDAP

<http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf>

LDAP Implementation Cookbook Este libro está dirigido especialmente a administradores de *IBM SecureWay Directory*. No obstante, también contiene información general sobre LDAP

<http://www.redbooks.ibm.com/redbooks/pdfs/sg245110.pdf>

Bibliografía impresa (en inglés) sobre LDAP:

- Howes, Smith & Good: *Understanding and Deploying LDAP Directory Services*. Addison-Wesley, 2. Aufl., 2003. - (ISBN 0-672-32316-8)
- Hodges: *LDAP System Administration*. O'Reilly & Associates, 2003. - (ISBN 1-56592-491-6)

NIS – Network Information Service

Cuando en una red existen varios sistemas Unix que quieren acceder a recursos comunes, hay que garantizar la armonía de las identidades de usuarios y de grupos en todos los ordenadores de la red. La red debe ser completamente transparente para el usuario; independientemente del ordenador en que trabaje, el usuario siempre debe encontrar el mismo entorno, lo cual se consigue mediante los servicios NIS y NFS. Éste último sirve para la distribución de sistemas de archivos en la red y se describe en el apartado [NFS – Sistema de archivos distribuidos](#) en la página 382.

NIS (ingl. *Network Information Service*), se puede entender como un servicio de base de datos que proporciona acceso a los archivos `/etc/passwd`, `/etc/shadow` o `/etc/group` en toda la red. NIS puede prestar también servicios adicionales, p. ej. para `/etc/hosts` o `/etc/services`, pero estos no son objeto de discusión aquí. Muchas veces se usan las letras ‘YP’ como sinónimo para NIS; ésta es la abreviatura de *Yellow Pages*, es decir, las *páginas amarillas* en la red.

Servidores NIS: maestro y esclavo

Para realizar la instalación, escoja en Y_aST la opción ‘Servicios de red’ y allí ‘Servidor NIS’. En caso de que aún no exista ningún servidor NIS en su red, en la máscara que aparece a continuación debe activar el punto ‘Configurar un servidor maestro NIS’. En caso de que ya exista un servidor NIS (es decir, un “master”), puede añadir un servidor esclavo NIS (p. ej. si quiere configurar una nueva subred). Lo primero que se detalla es la configuración del servidor maestro. En caso de que alguno de los paquetes necesarios no esté instalado, Y_aST le pedirá que introduzca el CD o DVD correspondiente para que los paquetes que faltan puedan instalarse automáticamente. En la primera máscara de configuración (figura 13.13 en la página siguiente), introduzca arriba el nombre del dominio. En la casilla inferior puede establecer si el ordenador también debe ser un cliente NIS, es decir si los usuarios pueden realizar logins y por tanto acceder a los datos del servidor NIS.

Si quiere configurar servidores esclavos NIS (“slave”) adicionales, debe activar la casilla ‘Disponer de servidor esclavo activo para NIS’. Además también debe activar ‘Distribución rápida de mapeo’, lo cual provoca que las entradas de la base de datos se envíen rápidamente del servidor maestro al esclavo.

Si quiere que los usuarios de la red puedan cambiar sus contraseñas (con el comando `yppasswd`, no sólo las locales sino también las que se encuentran en el servidor NIS), puede activar esta opción aquí.



Figura 13.13: YaST: Herramienta de configuración de un servidor NIS

Al hacerlo también se activarán las opciones ‘Permitir el cambio de GECOS’ y ‘Permitir el cambio de SHELL’. “GECOS” significa que el usuario también puede modificar su nombre y dirección (con el comando `ypchfn`). “SHELL” quiere decir que también puede modificar su shell (con el comando `ypchsh`, p. ej. de `bash` a `sh`).

Pulsando en el apartado ‘Otras configuraciones globales...’ accede a un diálogo (Figura 13.14 en la página siguiente) en el que puede modificar el directorio fuente del servidor NIS (por defecto `/etc`). Además aquí también se pueden reunir contraseñas y grupos. La configuración se debe dejar en ‘Sí’, para que los archivos correspondientes (`/etc/passwd` y `/etc/shadow`, o bien `/etc/group` y `/etc/gshadow`) concuerden mutuamente. Además se puede establecer el número más pequeño de usuarios y grupos. Con ‘OK’ confirma las entradas realizadas y vuelve a la máscara anterior. Pulse ahora en ‘Siguiente’.

Si ya ha activado ‘Disponer de servidor esclavo activo para NIS’, ahora debe introducir el nombre del ordenador que hará las veces de esclavo. Tras dar el nombre, diríjase a ‘Siguiente’.

También puede acceder directamente al menú que aparece a continuación si no ha activado la configuración del servidor esclavo. A continuación se pueden especificar los “maps”, es decir, las bases de datos parciales que se deben enviar del servidor NIS al cliente correspondiente.

En la mayoría de los casos pueden usarse las configuraciones predeterminadas.

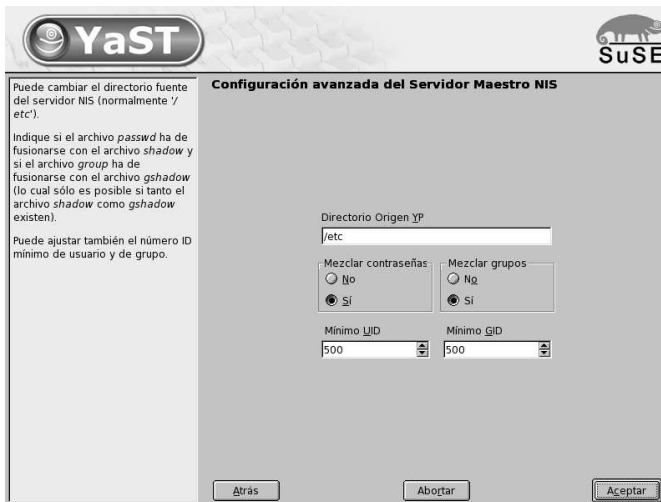


Figura 13.14: YaST: Servidor NIS: Cambiar directorios y sincronizar archivos

Por eso, en los casos normales no se debe cambiar nada. Para realizar modificaciones ha de ser un gran conocedor de la materia.

Con 'Siguiente' se llega al último diálogo en el que se puede determinar qué redes pueden realizar consultas al servidor NIS (ver Fig. 13.15 en la página siguiente). Normalmente se tratará de la red de su empresa, por lo que deberá introducir las entradas:

```
255.0.0.0 127.0.0.0
0.0.0.0 0.0.0.0
```

La primera permite las conexiones desde el propio ordenador, mientras que la segunda posibilita que todos los ordenadores que tienen acceso a la red envíen solicitudes al servidor.

El módulo del cliente NIS en YaST

Este módulo le permite configurar fácilmente el cliente NIS. Una vez que ha seleccionado en la máscara de inicio el uso de NIS y, en caso necesario, del automounter, pasará a la máscara siguiente. En ella ha de indicar si el cliente NIS tiene una dirección IP estática o si debe recibirla a través de DHCP. En este último caso no debe introducir el dominio NIS o la dirección IP del servidor, ya que estos datos serán también asignados a través de DHCP. Puede encontrar



Figura 13.15: YaST: Servidor NIS: Permiso de solicitud

información adicional sobre DHCP en el apartado [DHCP](#) en la página [387](#). Si el cliente dispone de una dirección IP fija, el dominio y el servidor NIS han de introducirse manualmente (ver Fig. [13.16](#) en la página siguiente) . Con el botón 'Buscar' YAST examinará la red en busca de un servidor NIS activo.

También puede añadir múltiples dominios con un dominio por defecto. Para cada dominio, con la opción 'Añadir' puede indicar más servidores e incluso la función broadcast.

En las opciones avanzadas de configuración puede evitar que otro ordenador de la red pregunte cuál es el servidor utilizado por su cliente. Al activar la opción 'Servidor roto' se aceptarán respuestas de un servidor en un puerto no privilegiado. Puede consultar información adicional sobre este tema en la página del manual de ypbind.



Figura 13.16: YaST: Cliente NIS

NFS – Sistema de archivos distribuidos

Como ya se ha mencionado en el apartado 13 en la página 377, el servicio NFS sirve, junto con el servicio NIS, para hacer una red transparente para el usuario. NFS permite la distribución de sistemas de archivos en la red, gracias a lo cual el usuario encuentra siempre el mismo entorno, independientemente del ordenador en el que trabaje.

Al igual que NIS, NFS es un servicio asimétrico de estructura cliente-servidor; pero a diferencia de éste, NFS puede ofrecer sistemas de archivos a la red ("exportar") y a su vez montar los de otros ordenadores ("importar"). La constelación más habitual consiste en utilizar servidores con discos duros de gran capacidad para exportar sistemas de archivos que serán montados por los clientes.

Importar sistemas de archivos con YaST

Todo usuario (al que le han asignado ciertos derechos) puede distribuir directorios NFS de servidores NFS en su propio árbol de directorios. Para ello, el método más sencillo consiste en utilizar el módulo 'Cliente NFS' de YaST. Allí se debe introducir el nombre de host del ordenador que hace las veces de servidor NFS, el directorio a exportar del servidor, y el punto de montaje en el que se debe montar en el ordenador. En la primera ventana de diálogo escoja 'Añadir' e introduzca la información mencionada (Fig. 13.17).

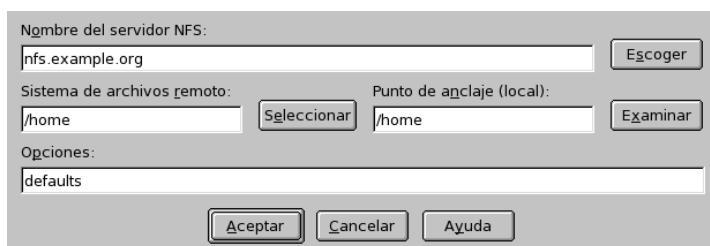
The image shows a graphical user interface window for configuring an NFS client. It has a light gray background and several input fields and buttons. At the top, there's a label 'Nombre del servidor NFS:' followed by a text box containing 'nfs.example.org' and a button labeled 'Elegir'. Below this, there are two columns. The left column has a label 'Sistema de archivos remoto:' and a text box with '/home', followed by a button 'Seleccionar'. The right column has a label 'Punto de anclaje (local):' and a text box with '/home', followed by a button 'Examinar'. At the bottom left, there's a label 'Opciones:' and a text box containing 'defaults'. At the very bottom, there are three buttons: 'Aceptar', 'Cancelar', and 'Ayuda'.

Figura 13.17: Configuración de un cliente NFS

Importar sistemas de archivos manualmente

Importar manualmente sistemas de archivos desde un servidor NFS es muy simple y tiene como única condición que el mapeador de puertos o

portmapper RPC. esté activo. Para iniciar este servidor, ejecute el comando `rportmap start` como usuario `root`. Una vez iniciado este servicio es posible incorporar sistemas de archivos externos al sistema de archivos local, siempre que puedan exportarse de las máquinas correspondientes. El procedimiento es análogo a la incorporación de discos locales usando el comando `mount`. La sintaxis del comando es la siguiente:

```
mount <ordenador>:<ruta remota> <ruta local>
```

Se pueden importar p. ej. los directorios de usuario del ordenador `sol` con el siguiente comando:

```
mount sol:/home /home
```

Exportar sistemas de archivos con YaST

Con YaST puede convertir rápidamente un ordenador de su red en un servidor NFS; en otras palabras, un servidor que pone archivos y directorios a disposición de todos los ordenadores a los que se haya otorgado acceso. Muchas aplicaciones pueden p. ej. estar disponible para los empleados sin que sea necesario instalarlas en sus PCs.

Para realizar la instalación, escoja en YaST la opción ‘Servicios de red’ y allí la opción ‘Servidor NFS’ (Fig. 13.18 en la página siguiente).

A continuación active la opción ‘Arrancar el servidor NFS’ y pulse en ‘Siguiente’. Ahora ya sólo queda introducir en la casilla superior los directorios que deben exportarse y en la inferior los ordenadores de la red a los que se les permite el acceso (figura 13.19 en la página 386). Existen cuatro opciones disponibles para los ordenadores: *<single host>*, *<netgroups>*, *<wildcards>* y *<IP networks>*. Puede encontrar una explicación más detallada de estas opciones en las páginas man del paquete `exports` (`man exports`).

Con ‘Finalizar’ cierra la ventana de configuración.

Exportar manualmente sistemas de archivos

Si prescindir del apoyo de YaST, asegúrese de que los siguientes servicios estén en funcionamiento en el servidor NFS:

- RPC-Portmapper (`portmap`)
- RPC-Mount-Daemon (`rpc.mountd`)
- RPC-NFS-Daemon (`rpc.nfsd`)



Figura 13.18: YaST: Herramienta de configuración de servidores NFS

Introduzca los comandos `insserv /etc/init.d/nfsserver` e `insserv /etc/init.d/portmap` para que los servicios sean activados por los scripts `/etc/init.d/portmap` y `/etc/init.d/nfsserver` al arrancar el ordenador.

Aparte de iniciar estos daemons es preciso definir qué sistemas de archivos se deben exportar a qué ordenadores. Esto se realiza con el archivo `/etc/exports`.

Por cada directorio a exportar se necesita una línea que defina qué ordenador debe acceder a él y de qué forma; los subdirectorios se exportan automáticamente. Los ordenadores con permiso de acceso se indican generalmente por sus nombres (con el nombre del dominio incluido). También puede usar los comodines `'*'` y `'?'` con sus funciones conocidas de la shell `bash`. Si no se indica ningún nombre, todos los ordenadores tienen la posibilidad de montar el directorio con los derechos de acceso indicados.

Los derechos con los que el directorio se exporta están indicados entre paréntesis en una lista detrás del nombre de ordenador. La siguiente tabla resume las opciones de acceso más importantes.

Opciones	Uso

Cuadro 13.15: Continúa en la página siguiente...

ro	Exportación sólo con derecho de lectura (por defecto).
rw	Exportación con derecho de escritura y lectura.
root_squash	Esta opción hace que el usuario <code>root</code> del ordenador indicado no tenga sobre el directorio los derechos especiales típicos para <code>root</code> . Esto se logra modificando los accesos con la identidad de usuario (ingl. <i>User-ID</i>) 0 al de 65534 (-2). Esta identidad debe estar asignada al usuario <code>nobody</code> (ésta es la opción por defecto).
no_root_squash	Ninguna modificación de los derechos de <code>root</code> .
link_relative	Modificación de enlaces simbólicos absolutos (aquellos que comienzan con '/') a una secuencia de './.'. Esta opción sólo tiene sentido si se monta el sistema de archivos completo de un ordenador (es así por defecto).
link_absolute	No se modifican los enlaces simbólicos.
map_identity	El cliente usa el mismo número de identificación (ingl. <i>User-ID</i>) que el servidor (ésta es la opción por defecto).
map_daemon	Los números de identificación de usuario, cliente y servidor no coinciden. Con esta opción, el <code>nfsd</code> genera una tabla para la conversión de los números de identificación de usuario. El requisito para ello es la activación del daemon <code>ugidd</code> .

Cuadro 13.15: *Derechos de acceso a directorios exportados*

El archivo 40 muestra un ejemplo de un archivo `exports`.

```
#
# /etc/exports
#
/home          sol(rw)   venus(rw)
/usr/X11       sol(ro)   venus(ro)
/usr/lib/texmf sol(ro)   venus(rw)
/              tierra(ro,root_squash)
/home/ftp      (ro)
# End of exports
```



Figura 13.19: YaST: Servidor NFS: Introducir el host y los directorios de exportación

Fichero 40: /etc/exports

Los programas mountd y nfsd leen el archivo /etc/exports. Después de haberlo modificado, es preciso reiniciar mountd y nfsd para que los cambios se activen. Para ello lo más sencillo es introducir el comando:

```
rcnfsserver restart
```

DHCP

El protocolo DHCP

El protocolo "Dynamic Host Configuration Protocol" tiene como función proporcionar configuraciones de forma centralizada desde un servidor de la red, evitando así el tener que hacerlo de forma descentralizada desde cada estación de trabajo. Un cliente que haya sido configurado con DHCP no posee direcciones estáticas sino que se configura totalmente de manera automática según las especificaciones del servidor DHCP.

Existe la posibilidad de identificar a un cliente mediante la dirección de hardware de su tarjeta de red y proporcionarle siempre la misma configuración, o bien de asignar dinámicamente direcciones de un depósito creado especialmente a los ordenadores "interesados". En este último caso, el servidor DHCP procurará asignar a un cliente siempre la misma dirección para cada consulta (aunque estén espaciadas en el tiempo) – claro que esto no funcionará si en la red hay más ordenadores que direcciones.

Por lo tanto, el administrador del sistema puede beneficiarse de DHCP de dos formas. Por una parte es posible realizar de forma centralizada, cómoda y automática grandes modificaciones (de configuración y/o de direcciones de red) en el archivo de configuración del servidor DHCP y todo ello sin tener que configurar los clientes uno a uno. Por otra parte y sobre todo, es posible integrar fácilmente nuevos ordenadores a la red asignándoles un número IP del conjunto de direcciones. En el caso de portátiles que operan de forma regular en varias redes, resulta muy útil la posibilidad de obtener la configuración de red correspondiente del respectivo servidor DHCP.

Además de asignar al cliente la dirección IP y la máscara de red se le entregarán también el nombre del ordenador y del dominio, la pasarela (gateway) a ser usada y las direcciones de los servidores de nombres.

Además también se pueden configurar de forma central algunos parámetros, como p. ej. un servidor de tiempo (ingl. *time server*), desde el cual se puede acceder a la hora actual

A continuación le ofrecemos una descripción a grandes rasgos del mundo de DHCP. También le mostraremos cómo realizar fácilmente la configuración de red de forma centralizada mediante DHCP y, más concretamente, con ayuda del servidor DHCP `dhcpcd`.

Los paquetes de software DHCP

SuSE Linux contiene un paquete de servidor DHCP y dos paquetes cliente. El servidor DHCP `dhcpcd` publicado por el Internet Software Consortium ofrece

los servicios de servidor. Como clientes DHCP disponemos de dos alternativas: por un lado, se encuentra `dhcpcd`, también realizado por ISC, y por el otro "DHCP Client Daemon", incluido en el paquete `dhcpcd`.

`dhcpcd` está incluido en la instalación estándar en SuSE Linux y su manejo es muy sencillo. Ya durante el arranque del ordenador éste se ejecuta de forma automática y busca un servidor DHCP. A `dhcpcd` no le hace falta un archivo de configuración y normalmente funciona sin ninguna configuración adicional.

Para situaciones más complejas se puede usar el `dhclient` de ISC, el cual se controla desde el archivo de configuración `/etc/dhclient.conf`

El servidor DHCP: `dhcpcd`

El *Dynamic Host Configuration Protocol Daemon* es el corazón de todo sistema DHCP. Éste se encarga de "alquilar" direcciones y de vigilar su uso como está estipulado en el archivo de configuración `/etc/dhcpd.conf`. El administrador del sistema puede determinar el comportamiento del DHCP según sus preferencias mediante los parámetros y valores definidos en este archivo.

Un ejemplo para un archivo `/etc/dhcpd.conf` sencillo:

```
default-lease-time 600;          # 10 minutes
max-lease-time 7200;             # 2  hours

option domain-name "cosmos.sol";
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;
}
```

Fichero 41: El archivo de configuración `/etc/dhcpd.conf`

Este sencillo archivo de configuración es suficiente para que DHCP pueda asignar direcciones IP en la red. Preste especial atención a los signos de punto y coma al final de cada línea sin los cuales `dhcpcd` no arrancará.

Como se puede observar, el anterior ejemplo puede dividirse en tres bloques. En la primera parte se define de forma estándar cuántos segundos se "alquilará"

una dirección IP a un ordenador que lo solicite antes de que éste tenga que pedir una prórroga (`default - lease - time`). Aquí también se define el tiempo máximo durante el cual un ordenador puede conservar un número IP otorgado por el servidor DHCP sin tener que tramitar para ello una prórroga (`max-lease-time`).

En el segundo bloque se definen globalmente algunos parámetros de red básicos:

- Con `option domain-name` se define el dominio por defecto de su red.
- En `option domain-name-servers` se pueden introducir hasta tres servidores DNS que se encargarán de resolver direcciones IP en nombres de host (y viceversa). Lo ideal sería que en su sistema o en su red hubiese ya un servidor de nombres en funcionamiento que proporcionase los nombres de host para las direcciones dinámicas y viceversa. Obtendrá más información sobre la creación de un propio servidor de nombres en el capítulo sobre DNS.
- `option broadcast-address` define qué dirección broadcast debe usar el ordenador que efectúa la consulta.
- `option routers` define dónde deben ser enviados los paquetes de datos que no pueden ser entregados en la red local (a causa de la dirección del host de origen y el host de destino así como de la máscara de subred). Este enrutador suele actuar como la pasarela a Internet en pequeñas redes.
- `option subnet-mask` proporciona al cliente la máscara de red a entregar.

Por debajo de esta configuración general se define una red con su máscara de subred. Por último basta con seleccionar el rango de direcciones utilizado por el daemon DHCP para asignar direcciones IP a clientes que lo consulten. Para el ejemplo dado, son todas las direcciones entre `192.168.1.10` y `192.168.1.20` y también en el rango de `192.168.1.100` hasta `192.168.1.200`.

Después de esta breve configuración, ya debería ser posible iniciar el daemon DHCP mediante el comando `rcdhcpd start`.

Por motivos de seguridad, el daemon DHCP se inicia por defecto en un entorno chroot en SuSE Linux. Para poder encontrar los archivos de configuración, es necesario copiarlos en el nuevo entorno. Esto sucede automáticamente con el comando `rcdhcpd start`.

Asimismo es posible controlar la sintaxis de la configuración mediante el comando `rcdhcpd check-syntax`. Si hay algún problema y el servidor da un error en lugar de indicar "done", el archivo `/var/log/messages` así como la consola 10 ((Control) + (Alt) + (F10)) ofrecen más información.

¡Enhorabuena! Ya tiene su propio servidor DHCP.

Ordenadores con direcciones IP fijas

Como ya se ha mencionado, también existe la posibilidad de asignar a un determinado ordenador la misma dirección IP en cada consulta.

Estas asignaciones explícitas de una dirección tienen prioridad sobre la asignación de direcciones desde un conjunto de direcciones dinámicas. Al contrario de lo que sucede con las direcciones dinámicas, las fijas no se pierden; ni siquiera cuando ya no quedan direcciones y se requiere una redistribución de las mismas.

Para identificar a los sistemas que deben obtener una dirección *estática*, `dhcpd` se sirve de la dirección de hardware. Ésta es una dirección única en el mundo para identificar las interfaces de red. Se compone de seis grupos de dos cifras hexadecimales, p. ej. `00:00:45:12:EE:F4`.

Al ampliar el archivo de configuración que se refleja en el extracto 41 en la página 388 con una entrada como se muestra en el extracto 42, `DHCPD` siempre entrega los mismos datos al ordenador correspondiente.

```
host tierra
  hardware ethernet 00:00:45:12:EE:F4;
  fixed-address 192.168.1.21;
```

Fichero 42: Ampliación del archivo de configuración

El significado de estas líneas se explica prácticamente por sí mismo:

Primero aparece el nombre del ordenador que se va a definir (host *hostname*) y en la línea siguiente se introduce la dirección MAC. Es muy fácil de averiguar en Linux ejecutando el comando `ifstatus` seguido de la interfaz de red (p. ej. `eth0`). Puede que sea necesario activar previamente la tarjeta: `ifup eth0`. Este comando produce una salida como: "link/ether 00:00:45:12:EE:F4".

Siguiendo el ejemplo expuesto, el ordenador con la dirección MAC

00:00:45:12:EE:F4 recibe automáticamente la dirección IP 192.168.1.21 y el nombre `tierra`.

Como tipo de hardware hoy en día se suele utilizar `ethernet`, pero tampoco hay problemas con `token-ring` que se encuentra en muchos sistemas de IBM.

Información adicional

Como se ha mencionado al principio, el capítulo no pretende más que introducir al lector en el mundo de DHCP. En la página web del *Internet Software Consortium* (<http://www.isc.org/products/DHCP/>) se encuentra información detallada sobre DHCP y sobre la versión 3 de este protocolo que actualmente se está desarrollando. Además existen las páginas `man dhcpd`, `man dhcpd.conf`, `man dhcpd.leases` y `man dhcp-options`. También hay una serie de libros en el mercado que detallan las posibilidades del *Dynamic Host Name Configuration Protocol*.

Otra característica interesante de `dhcpd` es la posibilidad de entregar un archivo con un kernel a los clientes que lo soliciten. Es algo que se define mediante el parámetro `filename` en el archivo de configuración. Así se pueden configurar clientes sin disco duro y cargar tanto el sistema operativo como los datos a través de la red, lo que puede resultar muy interesante por motivos económicos y de seguridad.

Sincronización horaria con xntp

Introducción

En muchos de los procesos que tienen lugar en un sistema informático, la hora exacta juega un papel primordial. Por este motivo, todos los ordenadores incorporan normalmente un reloj que desgraciadamente no siempre satisface los requisitos exigidos por aplicaciones tales como bases de datos. Entre las posibles soluciones se encuentra, por un lado, el ajustar el reloj local del ordenador constantemente o, por otro, el corregir periódicamente el reloj a través de la red. En el mejor de los casos, el reloj del ordenador no debe atrasarse nunca y los pasos realizados para adelantar el reloj no deben superar un intervalo de tiempo concreto. Comparativamente resulta mucho más sencillo ajustar el reloj de cuando en cuando con el programa `ntpdate`. No obstante, este proceso implica un salto importante en el tiempo que no todas las aplicaciones toleran.

`xntp` constituye un interesante planteamiento para resolver el problema. Por una parte, `xntp` corrige continuamente el reloj local del ordenador tomando como base los datos de corrección recopilados en el sistema. Por otra, utiliza servidores de tiempo en la red para corregir la hora local de forma permanente. Una tercera posibilidad consiste en administrar referentes locales de tiempo como relojes atómicos.

Configuración en red

Según la configuración predeterminada de `xntp` en SuSE Linux, el único referente de tiempo es el reloj local del ordenador. El modo más sencillo de utilizar un servidor de tiempo de la red es introduciendo el parámetro "server". Por ejemplo, si en la red existe un servidor de tiempo llamado `ntp.example.com`, podemos introducir dicho servidor en el archivo `/etc/ntp.conf` de esta forma:

```
server ntp.example.com
```

Para añadir servidores de tiempo adicionales se introducen líneas suplementarias con la palabra clave "server". Una hora después de iniciar `xntpd` con el comando `rcxntpd start`, el tiempo se estabiliza y se crea el archivo "drift-File" para corregir el reloj local del ordenador. La ventaja a largo plazo de "drift-File" radica en que al encender el ordenador se sabe ya cómo se desajusta el reloj de hardware con el tiempo. La corrección se activa entonces inmediatamente con lo que se consigue un tiempo de máquina muy estable.

Mientras sea posible acceder al servidor de tiempo en la red mediante una llamada general o broadcast, no necesita un servidor de nombres. Puede definir este proceso en el archivo de configuración `/etc/ntp.conf` con el parámetro `broadcastclient`. En este caso se recomienda configurar también los mecanismos de autenticación. De no ser así, un servidor de tiempo defectuoso en la red podría modificar su tiempo de máquina.

Por regla general, es posible dirigirse a cualquier `xntpd` en la red como a un servidor de tiempo. Para ejecutar `xntpd` también con broadcasts, utilice la opción `broadcast`:

```
broadcast 192.168.0.255
```

Aquí ha de sustituir la dirección de broadcast del ejemplo por la dirección pertinente en su caso. No obstante, asegúrese de que el servidor de tiempo utiliza la hora correcta. Para ello puede servirse, por ejemplo, de relojes de referencia.

Instalar un reloj de referencia local

El paquete `xntp` incluye controladores que permiten conectar relojes de referencia locales. Los relojes soportados se encuentran en el archivo <file:///usr/share/doc/packages/xntp-doc/html/refclock.htm> del paquete `xntp-doc`. A cada controlador se le ha asignado un número. La auténtica configuración se lleva a cabo en `xntp` a través de direcciones IP falsas. Los relojes se introducen en el archivo `/etc/ntp.conf` como si estuvieran disponibles en la red.

Para ello reciben direcciones IP especiales con el formato `127.127.t.u`. El valor `t` se toma del archivo mencionado arriba con la lista de relojes de referencia. `u` es el número de dispositivo, el cual es siempre 0 a no ser que utilice varios relojes del mismo tipo en su ordenador. Así, un `Type 8 Generic Reference Driver (PARSE)` posee la dirección IP falsa `127.127.8.0`.

Cada controlador dispone normalmente de parámetros especiales que definen la configuración con más detalle. El archivo <file:///usr/share/doc/packages/xntp-doc/html/refclock.htm> contiene un enlace a la página web de cada controlador donde se describen estos parámetros. Por poner un ejemplo, para los relojes de tipo 8 es necesario especificar un modo adicional que describe el reloj más exactamente. Así, el módulo `Conrad DCF77 receiver module` tiene el modo 5. También puede introducir la palabra clave `prefer` para que `xntp` tome este reloj como referente. Por consiguiente, la línea `server` completa de un "Conrad DCF77 receiver module" sería:

```
server 127.127.8.0 mode 5 prefer
```

Otros relojes siguen el mismo esquema. Una vez instalado el paquete `xntp-doc`, la documentación sobre `xntp` está disponible en su sistema en el directorio `/usr/share/doc/packages/xntp-doc/html`.

El servidor web Apache

¿Qué es un servidor web?

Servidor web

Un servidor web proporciona páginas HTML a los clientes que lo solicitan. Estas páginas pueden estar almacenadas en un directorio del servidor (páginas pasivas o estáticas) o ser generadas de nuevo como respuesta a una solicitud (contenidos activos).

HTTP

Los clientes suelen ser navegadores web como Konqueror o Mozilla. La comunicación entre el navegador y el servidor web se produce a través del protocolo de transferencia de hipertexto (*Hypertext Transfer Protocol*). Quien tenga interés puede consultar la versión actual de dicho protocolo (HTTP 1.1) en RFC 2068 y Update RFC 2616, los cuales se encuentran en la URL <http://www.w3.org>.

URLs

El cliente solicita una página al servidor a través de una URL. Por ejemplo:

<http://www.suse.com/index.html> Una URL se compone de:

- Un protocolo. Los protocolos de uso más extendido son
 - <http://> el protocolo HTTP.
 - <https://> una versión de HTTP codificada y más segura.

- `ftp://` File Transfer Protocol, para cargar y descargar archivos.
- Un dominio, en este caso `www.suse.com`. A su vez, el dominio puede subdividirse: la primera parte (`www`) hace referencia a un ordenador, la segunda `suse.com` es el auténtico dominio. La suma de ambas partes se conoce como FQDN (Fully Qualified Domain Name o nombre de dominio totalmente cualificado).
- Un recurso, en este caso `index.html`. Esta parte indica la ruta completa al recurso. Este recurso puede ser un archivo (como en este caso), un script CGI, una página de servidor de Java, etc.

La solicitud es reenviada al dominio (`www.suse.com`) por diversos mecanismos de Internet (p. ej. sistema de nombres de dominio DNS). Estos mecanismos reenvían el acceso a un dominio a uno o varios ordenadores responsables. El mismo Apache se encarga de proporcionar el recurso (la página `index.html` en nuestro ejemplo) de su directorio de archivos. En este caso, el archivo se encuentra en el nivel superior del directorio, pero también podría haber estado incluido en un subdirectorio como

`www.suse.com/business/services/support/index.html`

La ruta al archivo es relativa con respecto al documento raíz o *DocumentRoot*, el cual puede modificarse en los archivos de configuración. El procedimiento para ello se describe en la sección *DocumentRoot* en la página 405.

Reproducción automática de una página predeterminada

Indicar la página no es absolutamente necesario. Si no se especifica ninguna página, Apache añade automáticamente a la URL un nombre usual para tales páginas. El nombre más común para una página de este tipo es `index.html`. Es posible configurar este proceso en Apache y definir los nombres de páginas a tener en cuenta. El procedimiento correspondiente se explica en el apartado *DirectoryIndex* en la página 406.

En este caso basta con especificar

`http://www.suse.com`

para que el servidor proporcione la página

`http://www.suse.com/index.html`

¿Qué es Apache?

El servidor web de uso más extendido

Apache es el servidor web más usado en todo el mundo con una cuota de mercado superior al 60 % (según <http://www.netcraft.com>). En las aplicaciones web, Apache se combina frecuentemente con Linux, la base de datos MySQL y los lenguajes de programación PHP y Perl. Esta combinación se ha dado en llamar "LAMP".

Entre las virtudes de Apache cabe destacar:

Ampliable

Las funciones de Apache pueden expandirse mediante módulos. Por ejemplo, Apache es capaz de ejecutar scripts CGI en múltiples lenguajes de programación con ayuda de módulos.

Aquí no se trata sólo de Perl y PHP, sino también de otros muchos lenguajes de scripts como Python o Ruby. Además existen módulos que posibilitan, entre otras muchas cosas, la transmisión segura de los datos (Secure Sockets Layer, SSL), la autenticación de usuarios, el registro ampliado, etc.

Personalizable

Apache puede adaptarse a los requisitos y necesidades del usuario mediante módulos escritos por el propio usuario. No obstante, para ello se requiere un cierto nivel de conocimientos ;-)

Estable

Apache es software de código abierto u Open Source, por lo que su código ha sido examinado y perfeccionado por numerosos programadores. Este control garantiza que Apache esté libre de fallos en su mayor parte (en la medida en que esto es posible en el software). No obstante, no existe una certeza absoluta de que no se descubran nuevos agujeros de seguridad en el futuro. El apartado *Seguridad* en la página 421 incluye fuentes de información para problemas de seguridad así como los métodos para obtener ayuda.

Prestaciones

Apache soporta un amplio abanico de prestaciones muy útiles. Las más importantes se describen a continuación.

Máquinas virtuales (virtual hosts)

El soporte de máquinas virtuales significa que es posible manejar varias páginas web con una instancia de Apache en un único ordenador, si bien el servidor web se manifiesta como varios servidores web independientes de cara al usuario. Las máquinas virtuales pueden estar configuradas en distintas direcciones IP o "en función de los nombres". Así se evita el tener que adquirir y administrar ordenadores adicionales.

Reescritura flexible de URLs

Apache ofrece múltiples posibilidades para manipular y reescribir URLs (URL rewriting). Puede encontrar información adicional en la documentación sobre Apache.

Negociación de contenido (content negotiation)

En función de las prestaciones del cliente (navegador), Apache puede proporcionar una página web a la medida de ese cliente. Por ejemplo, en el caso de navegadores antiguos o aquellos que trabajen sólo en modo texto (como p. ej. Lynx), se entregará una versión simplificada de la página web sin tramas. Al proporcionar una versión de la página apropiada para cada navegador, es posible evitar la incompatibilidad entre muchos navegadores en lo que a JavaScript se refiere.

Flexibilidad en el tratamiento de errores

Al producirse un fallo (p. ej. una página no está disponible), es posible reaccionar de forma flexible y responder convenientemente. El modo de respuesta puede configurarse de forma activa por ejemplo mediante CGI.

Fundamentos

Cuando Apache procesa una solicitud, se puede haber definido uno o varios gestores o "handlers" en el archivo de configuración para llevar a cabo ese proceso. Los gestores pueden formar parte de Apache o bien ser módulos activados para procesar la solicitud, por lo que el proceso puede configurarse de manera muy

flexible. Además existe la posibilidad de integrar en Apache módulos propios para obtener un control aún mayor sobre la tramitación de solicitudes.

La modularización está aún más acentuada en la versión 2 de Apache. En ella, el servidor se ocupa de un número muy reducido de tareas mientras que el resto se realiza a través de módulos. Esto se lleva hasta tal punto que incluso el procesamiento de HTTP tiene lugar a través de módulos. Por lo tanto, Apache 2 no debe ser necesariamente un servidor web; también puede asumir otras tareas muy distintas a través de módulos diferentes. Un ejemplo es el servidor de correo Proof-of-Concept (POP3) como módulo basado en Apache.

Diferencias entre Apache 1.3 y Apache 2

Resumen

Las principales ventajas de Apache 2 con respecto a Apache 1.3 son las siguientes:

- El modo de ejecutar simultáneamente varias solicitudes. En el caso de Apache 2 pueden utilizarse hebras o threads y procesos. La administración de procesos se produce en un módulo propio, el módulo multiproceso o MPM. Apache 2 reacciona de forma distinta a las solicitudes dependiendo del MPM. Las diferencias se reflejan en el rendimiento y la utilización de los módulos. Este tema se describe con detalle más adelante.
- La organización interna de Apache ha mejorado considerablemente: ahora se utiliza una nueva librería base (Apache Portable Runtime, APR) como interfaz para las funciones del sistema y para la administración de memoria. Asimismo, módulos tan importantes y extendidos como `mod_gzip` (o su sucesor `mod_deflate`) y `mod_ssl`, que participan activamente en el tratamiento de solicitudes, están mucho mejor integrados en Apache.
- Apache 2 domina el protocolo de Internet IPv6.
- Ya existe un mecanismo mediante el cual los fabricantes de módulos pueden determinar el orden de carga de los mismos sin que el usuario tenga que ocuparse de ello. El orden de ejecución de los módulos es a menudo muy importante y antiguamente se determinaba en función del orden de carga. Así, un módulo que sólo permita el acceso a determinados recursos a los usuarios autenticados debe activarse en primer lugar para que los usuarios sin permisos de acceso no lleguen a ver las páginas.

- Las solicitudes a Apache y sus respuestas pueden procesarse con filtros.
- Soporte de archivos mayores que 2 GB (large file support o LFS) en sistemas de 32 bits.
- Algunos módulos nuevos sólo están disponibles para Apache 2.
- Mensajes de error en varios idiomas.

Ver también <http://httpd.apache.org/docs-2.0/de/>.

¿Qué es una hebra o thread?

Es una especie de proceso "light" que requiere menos recursos que un proceso normal. Por este motivo, el rendimiento aumenta cuando se usan threads en vez de procesos. El inconveniente radica en que las aplicaciones han de ser "thread-safe" para poder ejecutarse en un entorno de threads. Esto significa:

- Las funciones (o métodos en el caso de las aplicaciones orientadas a objetos) deben ser "reentrantes", , la función siempre debe producir el mismo resultado con los mismos datos de entrada independientemente de que esté siendo ejecutada por otras hebras al mismo tiempo. Por lo tanto, las funciones deben estar programadas de tal forma que puedan ser ejecutadas por varias hebras simultáneamente.
- El acceso a recursos (variables en su mayor parte) debe estar regulado de manera que no se produzcan conflictos entre las hebras ejecutándose paralelamente.

Hebras y procesos

Mientras Apache 1.3 siempre inicia un proceso propio para cada solicitud, Apache 2 puede ejecutar solicitudes como un proceso propio o en un modelo mixto formado por procesos y hebras. El MPM "prefork" se ocupa de la ejecución en forma de proceso y el MPM "worker" de la ejecución como hebra. Durante la instalación es posible indicar qué MPM desea utilizar (ver sección *Instalación* en la página siguiente).

El tercer modo, "perchild" aún se encuentra en una fase experimental y por eso (todavía) no se incluye en la instalación de SuSE Linux.

El inconveniente de usar Apache 2 es que no todos los módulos se han adaptado al modo thread-safe. Si tiene que utilizar un módulo que todavía no soporta las hebras deberá seguir trabajando con Apache 1.3 o bien emplear Apache 2 con el MPM "prefork".

Conclusión

¿Qué versión de Apache es la más adecuada? Si hasta ahora ha trabajado satisfactoriamente con Apache 1.3 y la disponibilidad de las páginas web es lo más importante en su caso, la migración no corre prisa. Lo mismo sucede si tiene que utilizar módulos que todavía no han sido adaptados a Apache 2.

En cambio, si el rendimiento desempeña un papel primordial en su caso o si necesita alguna de las nuevas prestaciones de Apache 2 (como p. ej. los filtros), puede plantearse la migración.

Otro argumento en favor de Apache 2 es que para esta versión existe un módulo de configuración de YaST con el que podrá definir muy fácilmente las opciones de configuración.

En cualquier caso siempre se recomienda comprobar cómo funciona la propia página web con Apache 2 en un sistema de prueba antes de implementarlo en un sistema productivo.

Instalación

Selección de paquetes en YaST

Para solicitudes simples basta con seleccionar el paquete Apache, pudiendo escoger entre el paquete `apache` (Apache 1.3) o el paquete `apache2` (Apache 2). Las ventajas e inconvenientes de ambas versiones se han descrito en la sección [Diferencias entre Apache 1.3 y Apache 2](#) en la página 399. Para quien no quiera o deba utilizar las nuevas prestaciones de Apache 2, instalar Apache 1.3 (paquete `apache`) es apostar sobre seguro.

Si se decide por paquete `apache2`, debe instalar también alguno de los paquetes MPM como el paquete `apache2-prefork` o el paquete `apache2-worker`. A la hora de seleccionar el MPM adecuado tenga en cuenta que el MPM worker con hebras no puede emplearse con el paquete `mod_php4`, ya que no todas las librerías utilizadas por el paquete `mod_php4` son "thread-safe".

Activar Apache

Apache no se inicia automáticamente a pesar de estar instalado. Para iniciar Apache es necesario activarlo en el editor de niveles de ejecución. Con el fin de que siempre se inicie automáticamente al arrancar el sistema, debe activar los niveles de ejecución 3 y 5 en el editor de niveles de ejecución. Puede comprobar si Apache está activo introduciendo la siguiente URL en un navegador

<http://localhost/>

Si Apache está activo y el paquete `apache-example-pages` o el paquete `apache2-example-pages` está instalado, podrá ver una página de prueba.

Módulos para contenidos activos

Para emplear contenidos activos sirviéndose de los módulos es necesario instalar también los módulos para los lenguajes de programación correspondientes. Estos son el paquete `mod_perl` para Perl, el paquete `mod_php4` para PHP y el paquete `mod_python` para Python, o en su caso los módulos respectivos para Apache 2.

El empleo de estos módulos se describe en la sección *Crear contenidos activos con módulos* en la página 413.

Paquetes suplementarios

De manera adicional se recomienda instalar la abundante documentación que se encuentra en el paquete `apache-doc` o en el paquete `apache2-doc`. Existe un alias (para saber lo que es eso consulte la sección *Configuración* en la página siguiente) para la documentación que proporciona un acceso directo a la misma a través de la URL <http://localhost/manual>.

Para desarrollar módulos propios para Apache o compilar módulos de terceros fabricantes es necesario instalar también el paquete `apache-devel` o el paquete `apache2-devel`, así como las herramientas de desarrollo correspondientes, como por ejemplo las herramientas `apxs` que se describen en el apartado *Instalación de módulos con Apxs* en esta página.

Instalación de módulos con Apxs

`apxs` o su equivalente para Apache2, `apxs2`, constituye una herramienta muy valiosa para los desarrolladores de módulos. Este programa permite compilar e instalar mediante un solo comando los módulos disponibles en forma de texto fuente (incluyendo los cambios necesarios en los archivos de configuración). También posibilita la instalación de módulos disponibles en forma de archivos de objetos (extensión `.o`) o librerías estáticas (extensión `.a`). A partir de las fuentes, `apxs` crea un objeto dinámico compartido (DSO) que puede ser utilizado directamente como módulo por Apache.

Con el siguiente comando se puede instalar un módulo a partir del texto fuente:

```
apxs -c -i -a mod_foo.c
```

Para ver opciones adicionales de `apxs`, consulte las páginas del manual.

En el apartado *Instalación* en la página 401 se describe qué paquetes deben ser instalados para que se instalen las distintas versiones de `apxs`.

Existen varias versiones de `apxs2`: `apxs2`, `apxs2-prefork` y `apxs2-worker`. Mientras que `apxs2` instala un módulo de tal forma que pueda usarse con todos los MPMs, los otros dos programas lo instalan de forma que sólo pueda ser usado por el MPM correspondiente ("prefork" o "worker"). `apxs2` instala los módulos en `/usr/lib/apache2`. En cambio, `apxs2-prefork` los instala en `/usr/lib/apache2-prefork`.

No se recomienda utilizar Apache 2 con la opción `-a`, ya que los cambios se escribirán directamente en `/etc/httpd/httpd.conf`. En su lugar, conviene activar los módulos a través de la entrada `APACHE_MODULES` en `/etc/sysconfig/apache2`, tal y como se describe en la sección *Configuración con SuSEconfig* en esta página.

Configuración

¿Debo configurar en absoluto?

Una vez instalado Apache, sólo es necesario configurarlo si se tienen requisitos o necesidades especiales. En la mayoría de los casos, Apache puede utilizarse tal y como está.

La configuración de Apache puede llevarse a cabo mediante `SuSEconfig`; o bien editando directamente el archivo `/etc/httpd/httpd.conf`. Si desea editar `/etc/httpd/httpd.conf` directamente, debe asignar el valor `no` a la entrada

```
ENABLE_SUSECONFIG_APACHE="yes"
```

en `/etc/sysconfig/apache2` con el fin de que `SuSEconfig` no sobrescriba los cambios efectuados en `/etc/httpd/httpd.conf`.

Configuración con SuSEconfig

Las opciones que puede definir en `/etc/sysconfig/apache` (y `/etc/sysconfig/apache2`) son integradas en los archivos de configuración de Apache por medio de `SuSEconfig`. Las posibilidades de configuración incluidas deberían bastar en la mayoría de los casos. En el archivo se encuentran comentarios explicativos sobre cada variable.

Archivos de configuración propios

En lugar de realizar los cambios directamente en el archivo de configuración `/etc/httpd/httpd.conf`, es posible definir un archivo de configuración propio mediante las variables `APACHE_CONF_INCLUDE_FILES` (por ejemplo `httpd.conf.local`, que será cargado posteriormente en el archivo de configuración principal. De este modo, los cambios efectuados en la configuración se mantienen aunque el archivo `/etc/httpd/httpd.conf` se sobrescriba al realizar una nueva instalación.

Módulos

Los módulos que han sido instalados con YQST se activan al asignar el valor "yes" a la variable correspondiente en `/etc/sysconfig/apache` (Apache 1.3) o bien introduciendo el nombre del módulo en la lista de la variable `APACHE_MODULES` (Apache 2). Esta variable se encuentra en el archivo `/etc/sysconfig/apache2`.

Flags

`APACHE_SERVER_FLAGS` permite introducir banderas que activan y desactivan secciones determinadas del archivo de configuración. Por ejemplo, si una sección del archivo de configuración se encuentra dentro de

```
<IfDefine someflag>
.
.
.
</IfDefine>
```

sólo está activada si la bandera correspondiente está definida en `ACTIVE_SERVER_FLAGS`:

```
ACTIVE_SERVER_FLAGS = ... someflag ...
```

De esta forma es posible activar y desactivar amplias secciones del archivo de configuración con fines de prueba.

Configuración manual

El archivo de configuración

El archivo de configuración `/etc/httpd/httpd.conf` (o bien `/etc/apache2/httpd.conf`) permite realizar cambios que no son posibles en la

configuración con `/etc/sysconfig/apache` o `/etc/sysconfig/apache2`. A continuación se indican algunos de los parámetros que puede definirse. Se explican aproximadamente en el mismo orden en el que aparecen en el archivo.

DocumentRoot

`DocumentRoot` es una opción básica de configuración. Se trata del directorio en el cual Apache aguarda las páginas web que han de ser proporcionadas por el servidor. Este directorio es `/srv/www/htdocs` para las máquinas virtuales predeterminadas y normalmente no debe ser modificado.

Timeout

Indica el periodo que el servidor espera antes de emitir la señal de tiempo agotado para una solicitud.

MaxClients

El número máximo de clientes para los que Apache puede trabajar simultáneamente. El valor predeterminado es 150, si bien este número puede resultar algo bajo para una página muy visitada. En el caso de Apache 1, este valor es modificado por `SuSEconfig` dependiendo del valor de la variable `HTTPD_PERFORMANCE`.

LoadModule

Las instrucciones `LoadModule` indican qué módulos se cargan. En Apache 1.3 la carga se produce en el orden en el que se han introducido las instrucciones `LoadModule`. El orden de carga en Apache 2 está definido a través de los mismos módulos (véase la sección *Diferencias entre Apache 1.3 y Apache 2* en la página 399).

Asimismo, estas instrucciones especifican los archivos incluidos en el módulo.

Port

Define el puerto en el que Apache aguarda las solicitudes. Éste es normalmente el puerto 80, que es el puerto estándar para HTTP. Por lo general no se recomienda modificar esta opción.

Por ejemplo, un posible motivo para que Apache esperase en otro puerto sería la prueba de la nueva versión de una página web. De esta forma, la versión activa de dicha página continuaría estando disponible en el puerto 80.

Otra razón sería el publicar páginas web con información confidencial disponible solamente en una red interna o intranet. Para ello se define, por ejemplo, el puerto 8080 y los accesos externos a este puerto se bloquean mediante el cortafuegos. De esta forma, el servidor está protegido de cara al exterior.

Directory

Mediante esta directiva se definen los permisos (por ejemplo de acceso) para un directorio. También existe una directiva de este tipo para `DocumentRoot`. El nombre de directorio indicado en esa directiva ha de concordar con el nombre indicado en `DocumentRoot`.

DirectoryIndex

Aquí pueden definirse los archivos que ha de buscar Apache para completar una URL cuando no se indica ningún archivo o recurso. El valor predeterminado es `index.html`. Por ejemplo, si el cliente solicita la URL

`http://www.xyz.com/foo/bar`

y en `DocumentRoot` se encuentra un directorio `foo/bar` que contiene un archivo llamado `index.html`, Apache proporciona esta página al cliente.

AllowOverride

Cualquier directorio del cual Apache obtenga documentos puede incluir un archivo que modifique para ese directorio los permisos de acceso y otras opciones definidas globalmente. Estas opciones de configuración se aplican recursivamente al directorio actual y a todos sus subdirectorios hasta que sean a su vez modificadas en un subdirectorio por otro de estos archivos. Esto significa que la configuración tiene validez global cuando se define en un archivo de `DocumentRoot`.

Estos archivos se llaman normalmente `.htaccess`, pero este nombre puede ser modificado (véase la sección [AccessFileName](#) en la página siguiente).

En `AllowOverride` se determina si la configuración definida en los archivos locales puede sobrescribir las opciones globales de configuración. Los valores admitidos para esta variable son `None` y `All` así como cualquier combinación posible de `Options`, `FileInfo`, `AuthConfig` y `Limit`. El significado de estos valores se describe con detalle en la documentación de Apache. El valor predeterminado (y más seguro) es `None`.

Order

Esta opción define el orden en el que se aplican las opciones de configuración para los permisos de acceso `Allow` y `Deny`. El valor predeterminado es:

`Order allow,deny`

Es decir, en primer lugar se aplican los permisos de acceso autorizados y a continuación los permisos de acceso denegados.

Los enfoques posibles son:

- "allow all" (permitir todos los accesos) más excepciones
- "deny all" (denegar todos los accesos) más excepciones

Un ejemplo del segundo enfoque:

```
Order deny,allow
Deny from all
Allow from example.com
Allow from 10.1.0.0/255.255.0.0
```

AccessFileName

Aquí es posible introducir los nombres de archivos que pueden sobrescribir las opciones globales de configuración en los directorios proporcionados por Apache (ver el apartado [AllowOverride](#) en la página anterior). El valor predeterminado es `.htaccess`.

ErrorLog

Esta opción contiene el nombre del archivo en el que Apache emite los mensajes de error. El valor predeterminado es `/var/log/httpd/errorlog`. Los mensajes de error para las máquinas virtuales (véase la sección [Máquinas virtuales](#) en la página 417) se emiten también en este archivo si no se ha especificado ningún archivo de registro propio en la sección correspondiente a la máquina virtual del archivo de configuración.

LogLevel

Dependiendo de su prioridad, los mensajes de error se agrupan en distintos niveles. Esta opción indica a partir de qué nivel de prioridad se emiten los mensajes de error. Sólo se emiten los mensajes con el nivel de prioridad introducido o superior. El valor predeterminado es `warn`.

Alias

Un alias define un atajo para un directorio que permite acceder directamente a dicho directorio. Por ejemplo, con el alias `/manual/` es posible acceder al directorio `/srv/www/htdocs/manual` aunque en `DocumentRoot` se haya definido otro directorio como `/srv/www/htdocs`. (Mientras el documento raíz tenga este valor, no hay ninguna diferencia.)

En el caso de este alias, con

```
http://localhost/manual
```

se puede acceder directamente al directorio correspondiente.

Para el directorio destino definido en una directiva `Alias` puede ser necesario crear una directiva `Directory` (véase la sección [Directory](#) en la página 406) en la que se definan los permisos para el directorio.

ScriptAlias

Esta instrucción se asemeja a `Alias`, pero indica además que los archivos del directorio destino han de ser tratados como scripts CGI.

Server Side Includes

Para activar estas opciones, las SSIs deben buscarse en todos los archivos ejecutables. Para ello se utiliza la instrucción

```
<IfModule mod_include.c>  
XBitHack on  
</IfModule>
```

Con el fin de poder buscar "Server Side Includes" en un archivo, el archivo en cuestión ha de hacerse ejecutable con

```
chmod +x <dateiname>
```

De manera alternativa, también es posible indicar explícitamente el tipo de archivo que ha de ser examinado en busca de SSIs. Esto se realiza con

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

No es una buena idea el introducir simplemente `.html`, ya que Apache examina entonces todas las páginas en busca de Server Side Includes (incluyendo aquellas que con seguridad no contienen ninguna), con la consiguiente disminución de rendimiento.

Estas instrucciones ya están incluidas en el archivo de configuración de SuSE Linux, por lo que normalmente no será necesario llevar a cabo ninguna configuración.

UserDir

Mediante el módulo `mod_userdir` y la directiva `UserDir` es posible definir un directorio dentro del directorio local de usuario en el que el usuario pueda publicar sus archivos a través de Apache. Esto se define en `SuSEconfig` mediante la variable `HTTPD_SEC_PUBLIC_HTML`. Para poder publicar archivos, la variable debe tener el valor `yes`. Esto conduce a la siguiente entrada en el archivo `/etc/httpd/suse_public_html.conf` (el cual es cargado por `/etc/httpd/httpd.conf`).

```
<IfModule mod_userdir.c>
    UserDir public_html
</IfModule>
```

Funcionamiento de Apache

¿Dónde se guardan las páginas y scripts?

Para mostrar sus propias páginas web (estáticas) con Apache basta con guardar los archivos en el directorio adecuado. En SuSE Linux éste es `/srv/www/htdocs`. Puede que el directorio ya contenga algunas páginas de ejemplo. El propósito de dichas páginas es probar después de la instalación si Apache ha sido instalado y funciona correctamente. Éstas pueden sobrescribirse sin problemas (o mejor aún, desinstalarse).

Los scripts CGI propios se guardan en `/srv/www/cgi-bin`.

Estado de Apache

Mientras está en funcionamiento, Apache escribe mensajes de registro en el archivo `/var/log/httpd/access_log` o bien `/var/log/apache2/`

`access_log`. Allí están documentados qué recursos con qué duración y qué método (GET, POST...) se han solicitado y proporcionado.

En caso de producirse fallos, encontrará la información correspondiente en el archivo `/var/log/httpd/error_log` (o `/var/log/apache2` en el caso de Apache2).

Contenidos activos

Información general

Apache ofrece varias posibilidades para proporcionar contenidos activos a clientes. Por contenidos activos se entienden páginas HTML creadas como resultado de datos variables introducidos por el cliente. Los buscadores constituyen un ejemplo muy conocido. En estas páginas, la introducción de uno o varios términos de búsqueda, quizá separados por operadores lógicos como "y", "o", etc., tiene como resultado una lista de páginas que incluyen el término buscado.

Existen tres formas de crear contenidos activos con Apache:

- **Server Side Includes (SSI).** Aquí se trata de instrucciones que son integradas en una página HTML por medio de comentarios especiales. Apache analiza el contenido de estos comentarios e incluye el resultado en la página HTML.
- **Common Gateway Interface (CGI).** En este caso se ejecutan programas situados dentro de determinados directorios. Apache pasa los parámetros transmitidos por el cliente a estos programas y devuelve el resultado de los programas al cliente. Este tipo de programación es relativamente fácil, especialmente al ser posible configurar programas de línea de comandos ya existentes para que acepten datos de entrada de Apache y emitan su salida a Apache.
- **Módulos.** Apache incluye interfaces para ejecutar cualquier módulo como parte del procesamiento de una solicitud y ofrece a estos programas acceso a información importante como la solicitud o la cabecera HTTP. De esta forma, en el procesamiento de solicitudes pueden participar programas que no sólo son capaces de crear contenidos activos sino también de realizar otras funciones (como p. ej. la autenticación).

La programación de estos módulos requiere un cierto nivel de conocimientos. Como contrapartida, se logra un alto rendimiento además de posibilidades más amplias que las obtenidas con SSI y CGI.

Comparación entre el intérprete de scripts como módulo y CGI

Mientras los scripts CGI se activan normalmente con una simple ejecución por parte de Apache (similar a la ejecución desde la línea de comandos), para utilizar los módulos es necesario integrar en Apache un intérprete que se ejecute continuamente. (Se dice que el intérprete es "persistente".)

De esta forma se evita el tener que iniciar y terminar un proceso propio para cada solicitud (lo que implica un importante consumo de recursos con respecto a la administración de procesos, gestión de memoria, etc.). En su lugar, el script se pasa al intérprete que ya está ejecutándose.

Este método tiene un inconveniente: Mientras los scripts ejecutados a través de CGI muestran una relativa tolerancia ante fallos de programación, dichos fallos tienen un efecto muy negativo cuando se utilizan módulos. La razón es que, en scripts CGI normales, los programas son finalizados tras procesar la solicitud y los fallos de recursos o memoria no compartidos no tienen tanta importancia porque la memoria o recurso vuelve a estar disponible una vez finalizado el programa.

En cambio, al utilizar los módulos, los efectos de los fallos de programación son permanentes ya que el intérprete está en constante ejecución. Si el servidor no es reiniciado, el intérprete puede funcionar sin interrupción durante meses. Durante un periodo tan largo, los recursos no compartidos se hacen notar...

SSI

Server Side Includes son instrucciones integradas en comentarios especiales ejecutados por Apache. El resultado se integra inmediatamente en la salida de Apache. Por ejemplo, la instrucción

```
<!--#echo var="DATE_LOCAL" -->
```

produce la fecha actual. Nótese aquí # inmediatamente después del inicio del comentario <!--, que indica a Apache de que se trata de una instrucción SSI y no de un comentario normal.

Las instrucciones SSIs pueden activarse de diversas maneras. El modo más sencillo consiste en examinar todos los archivos ejecutables en busca de Server Side Includes. La alternativa implica definir ciertos tipos de archivos que deben examinarse en busca de SSIs. Ambos procedimientos se explican en la sección *Server Side Includes* en la página 408.

CGI

¿Qué es CGI?

CGI es la abreviatura de “Common Gateway Interface”. Mediante CGI, el servidor no se limita a proporcionar una página HTML estática, sino que ejecuta un programa que se encarga de entregar esa página. De esta forma es posible crear páginas fruto de una operación de cálculo, como el resultado de una búsqueda en una base de datos. Además existe la posibilidad de pasar parámetros al programa ejecutado, permitiéndose así entregar una página individual de respuesta para cada solicitud.

Ventajas de CGI

La principal ventaja de CGI radica en su sencillez. El programa sólo tiene que estar en un directorio determinado para ser ejecutado por el servidor web como si se tratase de un programa en la línea de comandos. El servidor simplemente entrega al cliente el resultado del programa desde el canal estándar de salida (stdout).

GET y POST

Los parámetros de entrada pueden pasarse al servidor mediante GET o bien POST. Dependiendo del método utilizado, el servidor pasa los parámetros al script de forma distinta. En el caso de POST, el servidor pasa los parámetros al programa en el canal estándar de entrada (stdin) (el programa obtiene aquí los parámetros de la misma forma que si se iniciara en una consola).

Con GET, el servidor pasa los parámetros al programa en la variable de entorno QUERY_STRING. Una variable de entorno es una variable que el sistema pone a disposición general. Un ejemplo típico es la variable PATH, que contiene una lista de rutas que es examinada por el sistema en busca de comandos ejecutables cada vez que el usuario introduce un comando.

Lenguajes para CGI

En principio, los programas CGI pueden estar escritos en cualquier lenguaje de programación. Normalmente se utilizan lenguajes de scripts (lenguajes interpretados) como Perl o PHP. En el caso de CGIs que deban ejecutarse muy rápidamente, el lenguaje elegido será C o C++.

¿Dónde se guardan los scripts?

En el caso más sencillo, Apache espera a estos programas en un directorio concreto (`cgi-bin`). Este directorio puede definirse en el archivo de configuración, vea la sección [Configuración](#) en la página 403.

Asimismo es posible liberalizar varios directorios que Apache examina entonces en busca de programas ejecutables. No obstante esto conlleva cierto riesgo, ya que cualquier usuario (bien o malintencionado) será capaz de hacer que Apache ejecute programas. Si los programas ejecutables sólo se admiten en `cgi-bin`, el administrador puede controlar más fácilmente quién guarda qué programas o scripts en ese directorio y si dichos programas o scripts son peligrosos.

Crear contenidos activos con módulos

Módulos para lenguajes de scripts

Existen numerosos módulos que pueden utilizarse en Apache.

Atención

Módulos

El término "módulo" tiene aquí dos acepciones.

Por un lado se encuentran los módulos que pueden integrarse en Apache y que asumen en el servidor una función determinada como la integración de lenguajes de programación en Apache. Un ejemplo son los módulos que se explican a continuación.

Por otro lado, en los lenguajes de programación se emplea la palabra módulo para referirse a una cantidad determinada de funciones, clases y variables. Estos módulos se integran en programas para proporcionar diversas prestaciones. Un ejemplo son los módulos CGI disponibles en todos los lenguajes de scripts. Estos módulos simplifican la programación de aplicaciones CGI al ofrecer métodos para leer los parámetros de la solicitud y proporcionar código HTML.

Atención

SuSE Linux incorpora en forma de paquetes todos los módulos que se presentan a continuación.

mod_perl

Información general sobre Perl

Perl es un lenguaje de scripts muy utilizado y de eficacia probada. Existe una multitud de módulos y librerías para Perl (entre las que se encuentra una librería para ampliar el archivo de configuración de Apache). La página web de Perl es

<http://www.perl.com/>

Puede encontrar una amplia selección de librerías para Perl en la URL del proyecto Comprehensive Perl Archive Network (CPAN)

<http://www.cpan.org/>

Configurar mod_perl

Para trabajar con mod_perl en SuSE Linux, basta con instalar el paquete correspondiente (véase la sección *Instalación* en la página 401). Las entradas necesarias para Apache en el archivo de configuración ya están incluidas, véase /usr/include/apache/modules/perl/startup.perl (Apache 1) o bien /etc/apache2/mod\perl-startup.pl (Apache 2).

Puede obtener información adicional sobre mod_perl en:

<http://perl.apache.org/>

Contraposición de mod_perl y CGI

En el caso más sencillo, es posible ejecutar un script CGI como script mod_perl simplemente activándolo a través de otra URL. El archivo de configuración contiene alias que apuntan al mismo directorio y ejecutan los scripts allí almacenados a través de CGI o bien mediante mod_perl. Estas entradas ya han sido introducidas en el archivo de configuración.

La entrada alias para CGI es:

```
ScriptAlias /cgi-bin/ "/srv/www/cgi-bin/"
```

mientras que las entradas para mod_perl son las siguientes:

```
<IfModule mod_perl.c>
    # Provide two aliases to the same cgi-bin directory,
    # to see the effects of the 2 different mod_perl modes.
```

```
# for Apache::Registry Mode
ScriptAlias /perl/          "/srv/www/cgi-bin/"
# for Apache::Perlrun Mode
ScriptAlias /cgi-perl/      "/srv/www/cgi-bin/"
</IfModule>
```

Las siguientes entradas también son necesarias para `mod_perl` y se encuentran ya en el archivo de configuración.

```
#
# If mod_perl is activated, load configuration information
#
<IfModule mod_perl.c>
PerlRequire /usr/include/apache/modules/perl/startup.perl
PerlModule Apache::Registry

#
# set Apache::Registry Mode for /perl Alias
#
<Location /perl>
SetHandler perl-script
PerlHandler Apache::Registry
Options ExecCGI
PerlSendHeader On
</Location>

#
# set Apache::PerlRun Mode for /cgi-perl Alias
#
<Location /cgi-perl>
SetHandler perl-script
PerlHandler Apache::PerlRun
Options ExecCGI
PerlSendHeader On
</Location>

</IfModule>
```

Estas entradas crean nombres alias para los modos `Apache::Registry` y `Apache::PerlRun`. La diferencia entre ambos modos es la siguiente:

- En el caso de `Apache::Registry` se compilan todos los scripts y después se guardan en la memoria caché. Cada script se crea como contenido de una subrutina.

Aunque esto resulta positivo desde el punto de vista del rendimiento, presenta también un inconveniente: los scripts han de estar muy bien programados, ya que las variables y las subrutinas se mantienen entre los procesos de activación. Esto significa que las variables deben devolverse a su valor original para poder ser reutilizadas cuando se vuelva a activar el script. Por ejemplo, si se guarda el número de tarjeta de crédito de un cliente en un script de banca a distancia, este número podría volver a aparecer cuando el próximo cliente utilice la aplicación y vuelva a activar el script.

- `Apache::PerlRun` se comporta de manera semejante a CGI. Los scripts son compilados de nuevo para cada solicitud de tal forma que las variables y subrutinas desaparecen del espacio de nombres entre los procesos de activación. El espacio de nombres es el conjunto de todos los nombres de variables y rutinas definidos en un momento determinado durante la existencia de un script.)

Por tanto, con `Apache::PerlRun` no es necesario prestar tanta atención a la calidad de la programación, ya que todas las variables se inician al activar el programa y no pueden contener ningún valor procedente de procesos de activación anteriores.

Este es el motivo por el que `Apache::PerlRun` es más lento que `Apache::Registry`, pero aún así considerablemente más rápido que CGI, ya que se evita el tener que iniciar un proceso propio para el intérprete.

mod_php4

PHP es un lenguaje de programación creado especialmente para su uso con servidores web. Al contrario que otros lenguajes que guardan sus comandos en archivos independientes (scripts), los comandos en PHP están integrados en una página HTML de manera similar a SSI. El intérprete PHP procesa los comandos PHP e integra el resultado del proceso en la página HTML.

La página web de PHP es

<http://www.php.net/>

Paquetes: El paquete `mod_php4-core` ha de estar instalado necesariamente.

Para Apache 1 se requiere además el paquete `mod_php4` y para Apache 2 el paquete `apache2-mod_php4`.

mod_python

Python es un lenguaje de programación orientado a objetos con una sintaxis muy clara y legible. La estructura del programa depende del sangrado, lo cual puede resultar un poco raro al principio pero muy cómodo cuando uno se acostumbra. Los bloques no se definen por medio de abrazaderas (como en C y en Perl) o delimitadores como `begin` y `end`, sino mediante la profundidad del sangrado.

Puede encontrar información adicional sobre este lenguaje en

<http://www.python.org/>

y sobre `mod_python` en

<http://www.modpython.org/>

Puede instalarse el paquete `mod_python` o el paquete `apache2-mod_python`.

mod_ruby

Ruby

Ruby es un lenguaje de programación de alto nivel orientado a objetos. Ruby, un lenguaje relativamente joven, se asemeja tanto a Perl como a Python y resulta muy adecuado para su uso en scripts. Tiene en común con Python la sintaxis clara y bien organizada y con Perl las abreviaturas del tipo `$.r`, `emacs highlight fix`) y el número de la última línea leída del archivo de entrada. Ateniéndonos a su concepto, Ruby presenta enormes similitudes con Smalltalk.

La página web de Ruby es

<http://www.ruby-lang.org/>

Existe también un módulo Apache para Ruby cuya página web es

<http://www.modruby.net/>

Máquinas virtuales

Introducción a las máquinas virtuales

Las máquinas virtuales permiten poner en la red varios dominios con un único servidor web. De este modo se evitan los esfuerzos económicos y de administración derivados de contar con un servidor para cada dominio. Apache fue uno de los primeros servidores web en incluir esta característica y ofrece varias posibilidades para las máquinas virtuales:

- Máquinas virtuales en función del nombre
- Máquinas virtuales en función de la dirección IP
- Ejecución de varias instancias de Apache en un ordenador.

A continuación se explica más detalladamente cada una de las tres alternativas.

Máquinas virtuales en función del nombre

En el caso de las máquinas virtuales en función del nombre, una sola instancia de Apache se encarga de manejar varios dominios. Aquí no es necesario configurar varias direcciones IP para un ordenador. Ésta es la alternativa más sencilla y recomendable. Consulte la documentación de Apache para ver los posibles inconvenientes de la utilización de máquinas virtuales en función del nombre.

La configuración se realiza directamente en el archivo de configuración `/etc/httpd/httpd.conf`. Para activar las máquinas virtuales en función del nombre, es necesario introducir una directiva apropiada:

```
NameVirtualHost *
```

Aquí basta con introducir `*` para que Apache acepte todas las solicitudes entrantes.

A continuación debe configurarse cada una de las máquinas:

```
<VirtualHost *>
    ServerName www.empresa1.com
    DocumentRoot /srv/www/htdocs/empresa1.com
    ServerAdmin webmaster@empresa1.com
    ErrorLog /var/log/httpd/www.empresa1.com-error_log
    CustomLog /var/log/httpd/www.empresa1.com-access_log common
</VirtualHost>

<VirtualHost *>
    ServerName www.empresa2.com
    DocumentRoot /srv/www/htdocs/empresa2.com
    ServerAdmin webmaster@empresa2.com
    ErrorLog /var/log/httpd/www.empresa2.com-error_log
    CustomLog /var/log/httpd/www.empresa2.com-access_log common
</VirtualHost>
```

Nota: En este ejemplo y en los sucesivos, la ruta para los archivos de registro de Apache 2 debe cambiarse de `/var/log/httpd` a `/var/log/apache2`.

Para el dominio alojado originalmente por el servidor (www.empresa1.com) debe crearse también una entrada `VirtualHost`. En este ejemplo el servidor aloja, además del dominio original, un dominio adicional (www.empresa2.com).

En las directivas `VirtualHost` se introduce `*` al igual que en `NameVirtualHost`. Apache determina la conexión entre la solicitud y la máquina virtual mediante el campo `Host` en la cabecera HTTP. La solicitud es reenviada a la máquina virtual cuyo `ServerName` coincida con el nombre introducido en este campo.

En las directivas `ErrorLog` y `CustomLog` no es necesario que los archivos de registro contengan el nombre de dominio. Aquí es posible utilizar cualquier nombre.

`Serveradmin` representa la dirección de correo electrónico de un responsable con el que se puede contactar en caso de problemas. Si se producen errores, Apache incluye esta dirección en el mensaje de error que envía al cliente.

Máquinas virtuales en función de la dirección IP

Introducción

Con este método es necesario configurar varias direcciones IP en un ordenador. Una instancia de Apache maneja varios dominios, cada uno de los cuales tiene asignada una dirección IP. El siguiente ejemplo ilustra cómo se configura Apache de forma que, además de su dirección IP original `192.168.1.10`, aloje dos dominios adicionales en otras dos direcciones IP (`192.168.1.20` y `192.168.1.21`).

Este ejemplo concreto sólo funciona en una intranet, ya que las IPs del rango `192.168.0.0` a `192.168.255.0` no son reenviadas (enrutadas) en Internet.

Configuración de alias para direcciones IP

Con el fin de que Apache pueda alojar varias direcciones IPs, el ordenador en el que se ejecuta debe aceptar solicitudes para múltiples IPs, lo que se conoce como alojamiento de múltiples direcciones IP o multi-IP hosting.

Para ello es necesario en primer lugar activar el IP aliasing en el kernel. En SuSE Linux ya está activado de manera estándar.

Una vez que el kernel esté configurado para IP aliasing, ejecute como `root` los comandos `ifconfig` y `route` para configurar direcciones IP adicionales en el

ordenador. En el ejemplo que se presenta a continuación, el ordenador ya tiene una dirección IP propia, 192.168.1.10, que ha sido asignada al dispositivo de red eth0.

El comando `ifconfig` le permite determinar la dirección IP utilizada por el ordenador. Puede añadir direcciones IP adicionales p. ej.con

```
/sbin/ifconfig eth0:0 192.168.1.20
/sbin/ifconfig eth0:1 192.168.1.21
```

Todas estas direcciones IP están asignadas al mismo dispositivo físico de red (eth0).

Máquinas virtuales con IPs

Una vez que se ha configurado el IP aliasing en el sistema o el ordenador dispone de varias tarjetas de red, la configuración de Apache puede comenzar. En primer lugar se introduce un bloque `VirtualHost` para cada servidor virtual:

```
<VirtualHost 192.168.1.20>
    ServerName www.empresa2.com
    DocumentRoot /srv/www/htdocs/empresa2.com
    ServerAdmin webmaster@empresa2.com
    ErrorLog /var/log/httpd/www.empresa2.com-error_log
    CustomLog /var/log/httpd/www.empresa2.com-access_log common
</VirtualHost>

<VirtualHost 192.168.1.21>
    ServerName www.empresa3.com
    DocumentRoot /srv/www/htdocs/empresa3.com
    ServerAdmin webmaster@empresa3.com
    ErrorLog /var/log/httpd/www.empresa3.com-error_log
    CustomLog /var/log/httpd/www.empresa3.com-access_log common
</VirtualHost>
```

Aquí se introducen directivas `VirtualHost` sólo para los dominios adicionales, ya que el dominio original (www.empresa1.com) se configura mediante las opciones correspondientes (`DocumentRoot`, etc.) fuera de los bloques `VirtualHost`.

Múltiples instancias de Apache

En los dos métodos anteriores para las máquinas virtuales, los administradores de un dominio pueden leer los datos de los demás dominios. Para separar los dominios entre sí, es posible iniciar varias instancias de Apache, cada una de las cuales utiliza sus propias opciones de configuración para `user`, `group`, etc. en el archivo de configuración.

La directiva `Listen` indica en el archivo de configuración qué instancia de Apache está a cargo de qué dirección IP. Continuando con el ejemplo anterior, la directiva para la primera instancia de Apache es:

```
Listen 192.168.1.10:80
```

y para las otras dos instancias:

```
Listen 192.168.1.20:80
```

o bien

```
Listen 192.168.1.21:80
```

Seguridad

El método más seguro: ningún servidor

Si no se requiere ningún servidor web en el ordenador, se recomienda desactivar Apache en el editor de niveles de ejecución o no instalarlo siquiera (o bien desinstalarlo). Un servidor menos en el ordenador es un punto vulnerable menos para posibles ataques.

Esto tiene validez sobre todo para los ordenadores con función de cortafuegos, en los que si es posible nunca debería ejecutarse ningún servidor.

Permisos de acceso

`DocumentRoot` pertenece a `root`

Por defecto, los directorios `DocumentRoot` (`/srv/www/htdocs`) y `CGI` pertenecen al usuario `root` y se recomienda no modificar esta configuración. Si todos tuviesen permiso de escritura sobre estos directorios, cualquier usuario

sería capaz de guardar archivos en ellos. Estos archivos son ejecutados por Apache como usuario `wwwrun`. Apache no debería tener permisos de escritura sobre los datos y scripts que entrega, por lo que éstos no han de pertenecer al usuario `wwwrun`, sino por ejemplo a `root`.

Si se desea que los usuarios puedan guardar archivos en el directorio de documentos de Apache, se recomienda crear un subdirectorio en el que cualquiera pueda escribir, p. ej. `/srv/www/htdocs/usuarios`, en lugar de conceder permisos de escritura para el directorio de Apache.

Publicar documentos del propio directorio local de usuario

Otra posibilidad para que los usuarios puedan publicar en la red sus propios archivos consiste en introducir en el archivo de configuración un directorio local de un usuario en el que éste guarde sus archivos para la red (p. ej. `~/public_html`). Esta posibilidad, activada por defecto en SuSE Linux, se explica con más detalle en el apartado *UserDir* en la página 409.

Puede acceder a estas páginas web introduciendo el usuario en la URL: la URL contiene la expresión *nombre-usuario* como abreviatura del directorio correspondiente en el directorio local del usuario. Por ejemplo, al introducir en un navegador la URL

`http://localhost/~tux`

se muestran los archivos del directorio `public_html` situado en el directorio local del usuario `tux`.

Siempre al día

Quien administre un servidor web (sobre todo si dicho servidor está disponible públicamente), debe estar siempre informado y al día en lo que se refiere a fallos y posibles puntos vulnerables derivados de éstos.

En el apartado *Seguridad* en la página 424 se incluyen algunas fuentes de información sobre exploits y correcciones.

Identificación y resolución de problemas

¿Qué hacer cuando se presenta un problema? Por ejemplo: Apache muestra una página incorrectamente o no la muestra en absoluto.

- En primer lugar consultar el registro de errores: puede que el problema pueda deducirse de un mensaje de error allí presente. El archivo de registro de errores se encuentra en

`/var/log/httpd/error_log` bzw. `/var/log/apache2/error_log`.

Se recomienda mostrar los archivos de registro en una consola mientras se accede al servidor para ver cómo reacciona éste en cada momento. Con este fin, ejecute en una consola el siguiente comando como `root`:

```
tail -f /var/log/apache2/*_log
```

Esto también puede resultar muy útil cuando se presentan problemas al iniciar el servidor.

- Consulte la base de datos de fallos en la página web
<http://bugs.apache.org/>
- Examine las listas de correo y los foros de noticias. La lista de correo para los usuarios de Apache está disponible en
<http://httpd.apache.org/userslist.html>
En cuanto a los foros de noticias, se recomienda `comp.infosystems.www.servers.unix` y foros relacionados.
- Si no ha encontrado la información que buscaba en las fuentes anteriormente mencionadas y todavía está seguro de haber encontrado un fallo en Apache, puede informar de ello en
<http://www.suse.com/feedback/>

Documentación adicional

Apache

Apache dispone de abundante documentación que puede instalar como se describe en el apartado *Instalación* en la página 401. Una vez instalada, la documentación está disponible en

<http://localhost/manual>

La documentación más actual se encuentra siempre en la página web de Apache (en inglés):

<http://httpd.apache.org>

CGI

Puede encontrar información adicional (en inglés) sobre CGI en:

- <http://apache.perl.org/>
- <http://perl.apache.org/>
- <http://www.modperl.com/>
- <http://www.modpercookbook.org/>
- <http://www.fastcgi.com/>
- <http://www.boutell.com/cgic/>

Seguridad

La página

<http://www.suse.com/security/>

contiene los parches actuales para los paquetes de SuSE. Se recomienda visitar esta URL periódicamente o bien suscribirse a la lista de correo de anuncios de seguridad de SuSE.

El equipo de Apache es partidario de una política de información transparente en lo que se refiere a los fallos en Apache. La siguiente página contiene información actual sobre fallos encontrados y posibles puntos débiles derivados de los mismos:

http://httpd.apache.org/security_report.html

Si cree haber encontrado un problema de seguridad nuevo (por favor, compruebe siempre en las páginas mencionadas si se trata realmente de un problema nuevo), puede informar de él por correo electrónico a

security@suse.com

Puede obtener más información (en inglés) sobre problemas de seguridad en Apache y en otros programas de Internet en:

- <http://www.cert.org/>
- <http://www.vnunet.com/>
- <http://www.securityfocus.com/>

Fuentes adicionales

En caso de problemas le recomendamos consultar la base de datos de soporte de SuSE:

<http://sdb.suse.com/>

La siguiente URL contiene un periódico en línea sobre Apache

<http://www.apacheweek.com/>

La historia de Apache está explicada en

http://httpd.apache.org/ABOUT_APACHE.html

Esta página contiene datos muy interesantes, como por ejemplo por qué el servidor se llama "Apache".

Sincronización de ficheros

Hoy en día son muchas las personas que utilizan varios ordenadores: un ordenador en casa, otro en la oficina e incluso puede que un portátil o un PDA para los viajes. Algunos ficheros se necesitan en todos los ordenadores. Lo ideal sería poder trabajar con todos ellos y especialmente modificar los ficheros, pero que todos los ordenadores contuvieran la versión actual de los datos.

Software para sincronizar datos	428
Criterios para la elección de programa	430
Introducción a InterMezzo	434
Introducción a unison	437
Introducción a CVS	439
Introducción a mailsync	442

Software para sincronizar datos

La sincronización de datos no supone ningún problema en ordenadores que estén conectados entre sí permanentemente a través de una red rápida. Basta con elegir un sistema de ficheros de red como NFS y guardar los ficheros en un servidor. De esta forma, todos los ordenadores accederán a los mismos datos a través de la red.

Este planteamiento no es posible si la conexión en red es mala o parcialmente inexistente. Quien viaje con un ordenador portátil deberá tener copias de todos los ficheros que necesite en el disco duro local. No obstante, cuando los ficheros son editados no tarda en surgir el problema de la sincronización. Al modificar un fichero en un ordenador debe intentarse actualizar la copia de ese fichero en los demás ordenadores. Esto puede realizarse manualmente con ayuda de `scp` o `rsync` en caso de que se trate de pocas copias. Pero con un número elevado de ficheros resulta un proceso muy laborioso que requiere mucha atención por parte del usuario para no cometer fallos como, por ejemplo, sobrescribir un nuevo fichero con uno antiguo.

Aviso

Peligro de pérdida de datos

En cualquier caso hay que familiarizarse con el programa utilizado y probar su funcionamiento antes de administrar los propios datos a través de un sistema de sincronización. En caso de ficheros importantes resulta indispensable hacer antes una copia de seguridad.

Aviso

Para evitar el procedimiento largo y propenso a fallos de la sincronización manual de datos, existe software que, basándose en distintos planteamientos, se encarga de automatizar este proceso.

El soporte de instalación de SuSE NO cubre los programas descritos en este capítulo. El propósito de las breves descripciones que aparecen a continuación es simplemente dar al usuario una ligera idea sobre el funcionamiento de estos programas y cómo pueden ser utilizados. En caso de querer aplicar estos programas, le recomendamos leer atentamente la documentación de los mismos.

Inter-Mezzo

La idea de Intermezzo consiste en construir un sistema de ficheros que, como NFS intercambie ficheros a través de la red, pero que al mismo tiempo guarde copias locales en cada ordenador para que los ficheros estén disponibles aún

cuando no exista la conexión de red. Las copias locales pueden editarse y los cambios se almacenan en un fichero especial de registro. Cuando la conexión se restablece, los cambios se pasan automáticamente a los demás ordenadores y los ficheros son sincronizados. Si el paquete está instalado, puede encontrar más información sobre el programa InterMezzo en </usr/share/doc/packages/InterMezzo/InterMezzo-HOWTO.html>.

unison

En el caso de unison no se trata de un sistema de ficheros, sino que los ficheros se guardan y editan normalmente de forma local. El programa unison puede ejecutarse manualmente para sincronizar ficheros. Durante la primera sincronización, se crea en cada una de las dos máquinas participantes una base de datos en la que se recogen la suma de control, marca de tiempo y permisos de los ficheros seleccionados.

La próxima vez que se ejecute, unison reconoce qué ficheros han sido modificados y sugiere la transferencia de datos de uno u otro ordenador. En el mejor de los casos es posible aceptar todas las sugerencias.

CVS

CVS se utiliza sobre todo para administrar versiones de textos fuente de programas y ofrece la posibilidad de guardar copias de ficheros en distintos ordenadores, por lo que también resulta adecuado para la sincronización.

En el caso de CVS existe una base de datos central o repositorio (repository) en el servidor que no sólo guarda los ficheros sino también los cambios realizados en ellos. Las modificaciones efectuadas localmente pueden enviarse al repositorio (commit) y ser recogidos por otros ordenadores (update). Ambos procesos deben ser iniciados por el usuario.

CVS tolera muchos fallos en lo que se refiere a cambios en varios ordenadores. Así, los cambios son fusionados y sólo se produce un conflicto si se han realizado cambios en la misma línea. En caso de conflicto, los datos en el repositorio mantienen su coherencia y el conflicto sólo es visible y puede resolverse en el cliente.

mailsync

A diferencia de las herramientas de sincronización mencionadas hasta ahora, mailsync se ocupa únicamente de sincronizar mensajes entre varios buzones de

correo. Puede tratarse de ficheros de buzones locales o de buzones ubicados en un servidor IMAP.

Dependiendo del "message ID" incluido en la cabecera de cada mensaje, se decide individualmente si éste ha de borrarse o ser sincronizado.

Se permite la sincronización tanto entre buzones sueltos como entre jerarquías de buzones.

Criterios para la elección de programa

Cliente-servidor o igualdad de derechos

Existen dos modelos diferentes para la distribución de datos. Por un lado, es posible utilizar un servidor central con el que el resto de ordenadores ("clientes") compare sus ficheros. Para ello, todos los clientes han de poder acceder al servidor, por lo menos de vez en cuando, a través de una red. Este modelo es el utilizado por CVS e Intermezzo.

La alternativa consiste en que todos los ordenadores tengan los mismos derechos y comparen sus datos entre sí. Éste es el planteamiento empleado por unison.

Portabilidad

InterMezzo es una solución que hoy en día sólo funciona en sistemas Linux. Anteriormente estuvo incluso limitada a arquitecturas de 32 bits con el bit menos significativo primero (ix86). Esta restricción ya no existe gracias a la sustitución del programa lento basado en perl por InterSync. No obstante, se recomienda precaución a la hora de sincronizar entre distintas arquitecturas, ya que esta función no ha sido probada en profundidad.

cvcs y unison están disponibles para muchos otros sistemas operativos, como es el caso de otros Unix y Windows.

Interactivo o automático

Con InterMezzo, la sincronización de datos se ejecuta normalmente de manera automática como proceso de fondo tan pronto como la conexión al servidor se establece. Sólo es necesario intervenir en caso de que se produzca algún conflicto.

La sincronización de datos en cvs y unison es iniciada por el usuario. Esto permite un mayor control sobre los ficheros que se van a sincronizar y una resolución más fácil de posibles conflictos. Por otra parte, puede suceder que la sincronización se lleve a cabo con demasiada poca frecuencia, lo que aumenta el riesgo de conflictos.

Velocidad

Debido a su carácter interactivo, unison y cvs parecen más lentos que intermezzo, que funciona en segundo plano. En conjunto, cvs es algo más rápido que unison.

Conflictos: cuando aparecen y cómo resolverlos

En cvs aparecen conflictos rara vez, incluso aunque varias personas trabajen en un gran proyecto de programa. Los distintos documentos se fusionan línea a línea y, en caso de que ocurra un conflicto, sólo afectará a un cliente. Por lo general, los conflictos en cvs se resuelven fácilmente.

Los conflictos en unison se notifican al usuario y el fichero se puede entonces excluir de la sincronización. Por otra parte, los cambios no se fusionan tan fácilmente como en cvs.

Debido al carácter no interactivo de InterMezzo, los conflictos no pueden resolverse fácilmente de forma interactiva. Cuando aparece algún conflicto, InterSync se interrumpe con un mensaje de error. En este caso, el administrador del sistema ha de intervenir y si es necesario transferir ficheros manualmente (rsync/scp) para obtener de nuevo un estado coherente.

Seleccionar y añadir ficheros

InterMezzo sincroniza sistemas completos de ficheros. Los nuevos ficheros añadidos aparecen automáticamente en los demás ordenadores.

En la opción de configuración más sencilla de unison se sincroniza un árbol completo de directorios. Los nuevos ficheros presentes en el árbol se incorporan automáticamente a la sincronización.

En el caso de CVS es necesario añadir explícitamente nuevos directorios y ficheros por medio de `cvsv add`. La consecuencia es un mayor control sobre los ficheros que van a formar parte de la sincronización. Por otra parte, los nuevos ficheros tienden a olvidarse; sobre todo si debido al número de ficheros se ignora el signo '?' que aparece en la salida de `cvsv update`.

Historia

Como función adicional, cvs permite reconstruir las versiones anteriores de los ficheros. Cada vez que se realiza un cambio es posible añadir una pequeña nota y posteriormente reproducir el desarrollo del fichero basándose en el contenido y en los comentarios. Esto resulta de gran utilidad en el caso de tesis o textos de programas.

Cantidad de datos y requisitos de espacio

En cada uno de los ordenadores participantes se necesita espacio suficiente en el disco duro para todos los datos distribuidos.

En el caso de cvs se necesita además espacio adicional para la base de datos ("repository") en el servidor. Allí también se guarda la historia de los ficheros, por lo que los requisitos de espacio son mucho mayores que el espacio necesario en sí. En el caso de ficheros en formato texto, los requisitos de espacio se mantiene dentro de límites razonables, ya que sólo hay que volver a guardar las líneas que han sido modificadas. Pero en el caso de ficheros binarios, el espacio requerido aumenta en el orden del tamaño del fichero con cada cambio que se produce.

GUI

unison está equipado con una interfaz gráfica que muestra la sincronización sugerida por unison. Se puede aceptar esta propuesta o bien excluir ficheros sueltos del proceso de sincronización. Además es posible confirmar cada uno de los procesos de forma interactiva en modo texto.

Los usuarios más experimentados suelen utilizar cvs desde la línea de comandos. No obstante, también existen interfaces gráficas para Linux (cervisia, ...) y Windows (wincvs). Numerosas herramientas de desarrollo (ej. kdevelop) y editores de texto (ej. emacs) tienen soporte para CVS. A menudo, el uso de estas frontales simplifica en gran medida la resolución de conflictos.

El programa InterMezzo no es tan confortable. Por otra parte, normalmente no requiere ninguna interacción y, una vez configurado, sólo hay que dejarle ejecutarse en segundo plano.

Requisitos que debe cumplir el usuario

La configuración de InterMezzo es relativamente difícil y debe ser realizada por un administrador de sistemas con experiencia en Linux. Para configurar el programa son necesarios permisos `root`.

unison es muy fácil de usar y resulta adecuado también para usuarios principiantes.

El manejo de CVS es algo más complejo. Para utilizarlo es necesario haber comprendido la interacción entre el repositorio y los datos locales. Siempre hay que fusionar primero los cambios en los datos locales con el repositorio. Para ello se utiliza el comando `cvsv update`. Una vez hecho esto, los datos deben volver a enviarse al repositorio con `cvsv commit`. Siempre que se respeten estos procesos, el uso de CVS es muy sencillo incluso para principiantes.

Seguridad frente a agresiones externas

En un escenario ideal, la seguridad de la transferencia de datos debería estar garantizada en caso de accesos no autorizados o incluso de la modificación de los datos.

Tanto unison como cvs pueden utilizarse vía ssh (Secure Shell) y están por lo tanto bien protegidos frente a posibles agresiones como las mencionadas arriba. Se recomienda no utilizar cvs o unison a través de rsh (Remote Shell) y evitar también el acceso a través del mecanismo cvs "pserver" en redes poco protegidas.

En el caso de InterMezzo, la sincronización de datos se lleva a cabo a través de http, un protocolo que puede ser espiado o falsificado fácilmente. Para incrementar la seguridad puede utilizarse SSL, lo que por otra parte complica bastante la configuración. Sin el uso de SSL, InterMezzo sólo debe emplearse en redes protegidas y de confianza.

Seguridad frente a pérdida de datos

Numerosos desarrolladores utilizan desde hace mucho tiempo el excepcionalmente estable CVS para administrar sus proyectos de programación. Además, el almacenamiento de la historia de los cambios hace que en CVS se esté protegido incluso frente a determinados fallos del usuario (por ejemplo la eliminación accidental de un fichero).

unison es todavía relativamente nuevo, pero demuestra ya un alto grado de estabilidad. Es más sensible frente a fallos del usuario. Una vez confirmado un proceso de eliminación de un fichero durante la sincronización, no hay vuelta atrás.

Actualmente InterMezzo puede todavía calificarse como experimental. Debido a que los ficheros están almacenados en un sistema de ficheros subyacente, la probabilidad de perder los datos es bastante pequeña. No obstante, el proceso

	InterMezzo	unison	CVS	mailsync
CS/Igualdad	C-S	igualdad	C-S	igualdad
Portabilidad	Linux(i386)	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x
Interacción	-	x	x	-
Velocidad	++	-	o	+
Conflictos	-	o	++	+
Selecc.fich.	sist.fich.	directorio	selección	buzón
Historia	-	-	x	-
Esp. disco	o	o	-	+
GUI	-	+	o	-
Dificultad	-	+	o	o
Agresiones	-	+(ssh)	+(ssh)	+(SSL)
Pérdida datos	o	+	++	+

Cuadro 15.1: Características de las herramientas de sincronización de datos – = muy malo, - = malo o no disponible, o = regular, + = bueno, ++ = muy bueno, x = disponible

de sincronización en sí puede salir mal y producir como resultado ficheros defectuosos. La tolerancia a fallos del usuario es bastante reducida: la eliminación local de un fichero es reproducida por todos los ordenadores sincronizados. Por este motivo, se recomienda el uso de copias de seguridad.

Introducción a InterMezzo

Arquitectura

InterMezzo dispone de su propio tipo de sistema de ficheros. Los ficheros se guardan localmente en el disco duro de cada ordenador. Para ello se utiliza uno de los sistemas de ficheros Linux disponibles, preferiblemente `ext3` u otro de los sistemas de ficheros transaccionales. Después de preparar la partición, se monta el sistema de ficheros de tipo `intermezzo` y el kernel carga el módulo con soporte para InterMezzo. A partir de ese momento, todos los cambios que se realicen en este sistema de ficheros serán registrados en un fichero `log`.

Tras completar estas tareas preliminares, puede iniciarse InterSync. Éste a su vez inicia un servidor web, como por ejemplo `apache`, al que el resto de ordenadores puede acceder para intercambiar datos. Al configurar un cliente hay que informar a InterSync del nombre del servidor para que pueda establecer conexión

con él. Para detectar el sistema de ficheros se transmite una denominación arbitraria del sistema de ficheros, el llamado "fileset".

InterSync es una versión evolucionada del antiguo sistema InterMezzo, que utilizaba un daemon llamado lento escrito en perl para la sincronización de datos. En la documentación de InterSync aparecen a veces referencias a este antiguo sistema que ha sido sustituido completamente por InterSync. Desgraciadamente, el módulo incluido en el kernel estándar está aún al nivel de lento y no funciona con InterSync. El kernel SuSE contiene un nuevo módulo. En el caso de kernels de construcción propia, el módulo del kernel puede construirse con ayuda del paquete `km_intersync`.

Para la configuración de InterMezzo se requieren permisos root. Como se vió en la comparación, la configuración de InterMezzo es muy compleja y debe ser llevada a cabo por personas con un nivel de conocimientos equivalente al de un administrador de sistemas. La configuración que se describe a continuación no prevé ningún mecanismo de protección, por lo que es posible que alguien desde la red pueda espiar y modificar sin grandes dificultades los datos sincronizados a través de InterMezzo. Por este motivo, la instalación y configuración deberían tener lugar sólo en un entorno de confianza como por ejemplo una red por cable privada detrás de un cortafuegos.

Configuración de un servidor InterMezzo

El papel de servidor se le asigna a un ordenador que preferentemente tenga una buena conexión a la red. A través de este servidor discurrirá todo el tráfico para la sincronización de datos.

Para guardar los datos es necesario configurar un sistema de ficheros propio. Si ya no existe ninguna partición disponible y el usuario no utiliza LVM, la opción más fácil es crear el fichero en un dispositivo bucle ("loop device"). A través de este procedimiento, un fichero del sistema de ficheros local será considerado como sistema de ficheros propio.

En el siguiente ejemplo se describe la configuración de un sistema de ficheros InterMezzo/ext3 en el directorio root con un tamaño de 256MB. Al fileset se le asignará la denominación `fset0`.

```
dd if=/dev/zero of=/izo0 bs=1024 count=262144
mkizofs -r fset0 /izo0 # La advertencia puede ignorarse
```

Este sistema de ficheros será montado en `/var/cache/intermezzo`

```
mount -t intermezzo -o fileset=fset0,loop /izo /var/cache/intermezzo
```

Para que el proceso se lleve a cabo automáticamente durante el proceso de

arranque, debe añadirse una entrada en el fichero `/etc/fstab`. Ahora hay que configurar InterSync. Para ello es necesario adaptar el fichero `/etc/sysconfig/intersync`, para lo que se añaden las entradas

```
INTERSYNC_CLIENT_OPTS="--fset=fset0"  
INTERSYNC_CACHE=/var/cache/intermezzo  
INTERSYNC_PROXY=""
```

A continuación intersync puede iniciarse por medio del comando

```
/etc/init.d/intersync start
```

Para hacer que este proceso se realice automáticamente al iniciar el sistema, basta con introducir el servicio en la lista de los servicios que deben ser iniciados:

```
insserv intersync
```

Configuración de clientes InterMezzo

La configuración de los clientes (un servidor puede servir a numerosos clientes) apenas se distingue de la configuración del servidor. La única diferencia es que en la configuración de `/etc/sysconfig/intersync` es necesario introducir el nombre del servidor en la variable `INTERSYNC_CLIENT_OPTS`:

```
INTERSYNC_CLIENT_OPTS="-fset=fset0 -server=sol.cosmos.univ"
```

`sol.cosmos.univ` ha de sustituirse por el nombre de red del servidor. Además se recomienda crear un sistema de ficheros de igual tamaño en todos los ordenadores.

Resolución de problemas

En cuanto un cliente ha sido iniciado, los cambios realizados en ficheros pertenecientes al directorio `/var/cache/intermezzo/` deberían ser visibles también en el servidor y en los demás clientes. Si éste no es el caso, puede deberse a que no se ha podido establecer conexión con el servidor o a un fallo de configuración como que la denominación del "fileset" no coincide siempre. Para realizar el diagnóstico correspondiente se recomienda examinar los mensajes en el registro del sistema `/var/log/messages`. El servidor web iniciado lleva el registro de sus datos en `/var/intermezzo-X/`. El fichero log del kernel, el cual registra los cambios en el sistema de ficheros se encuentra en

`/var/cache/intermezzo/.intermezzo/fset0/kml` y puede volcarse con `kmlprint`.

En caso de conflictos, uno de los procesos de InterSync suele bloquearse. Si la sincronización de datos se ha detenido, se aconseja analizar los mensajes correspondientes en los ficheros de registro y comprobar por medio de `/etc/init.d/intersync status` si el servicio de sincronización todavía está en funcionamiento.

También puede consultarse la documentación del paquete:

`/usr/share/doc/packages/intersync/`
<http://www.inter-mezzo.org/>

Introducción a unison

Campos de aplicación

Unison resulta muy adecuado para la sincronización y transferencia de árboles de directorios completos. La sincronización se lleva a cabo de manera bidireccional y puede controlarse a través de un intuitivo frontal gráfico (también existe una versión para la consola). El proceso de sincronización puede automatizarse (es decir, sin necesidad de intervención por parte del usuario) si se poseen los suficientes conocimientos.

Requisitos

Unison debe estar instalado tanto en el servidor como en el cliente. Por servidor se entiende aquí un segundo ordenador remoto (al contrario que en el caso de CVS, véase el capítulo 6).

A continuación nos limitamos al uso de unison con ssh, por lo que en el cliente debe haber instalado un cliente ssh y en el servidor un servidor ssh.

Manejo

El principio básico de unison consiste en la unión de dos directorios (llamados "roots"). Esta unión no debe entenderse en sentido literal, no se trata por tanto de ninguna conexión. Asumiendo que tengamos la siguiente estructura de directorios:

Client: Server:
/home/tux/dir1 /home/geeko/dir2

Estos dos directorios han de ser sincronizados. En el cliente se conoce al usuario como **tux**, en el servidor como **geeko**. En primer lugar se comprueba si la comunicación entre cliente y servidor funciona:

```
unison -testserver /home/tux/dir1 ssh://geeko@server//homes/geeko/dir2
```

Los problemas más frecuentes que pueden aparecer a estas alturas son:

- las versiones de unison utilizadas en cliente y servidor no son compatibles
- el servidor no permite una conexión SSH
- las rutas introducidas no existen

Si todo funciona correctamente, se omite la opción `-testserver`.

Durante la primera sincronización, unison todavía no conoce el comportamiento de ambos directorios, por lo que sugiere el sentido de la transmisión de los ficheros y directorios individuales. La flecha en la columna "Action" define el sentido de la transmisión. El signo '?' significa que unison no puede hacer ninguna sugerencia sobre el sentido de transmisión porque ambas versiones son nuevas o porque entre tanto han sido modificadas.

Las teclas de cursor permiten definir el sentido de transmisión para cada entrada. Si los sentidos de transmisión para todas las entradas mostradas son correctos, pulse "Go".

El comportamiento de unison (por ejemplo, si la sincronización debe automatizarse en casos muy claros) puede controlarse mediante parámetros de la línea de comandos al iniciar el programa. La lista completa de todos los parámetros posibles puede consultarse con `unison -help`.

Para cada unión se lleva un registro en el directorio de usuario (`~/unison`). En este directorio también pueden guardarse conjuntos de configuración como `~/unison/example.prefs`:

```
root=/home/foobar/dir1
root=ssh://fbar@server//homes/fbar/dir2
batch=true
```

Fichero 43: El fichero `~/unison/example.prefs`

Para iniciar la sincronización, basta con introducir este fichero como argumento en la línea de comandos:

```
unison example.prefs
```

Información adicional

La documentación oficial de Unison es muy completa, por lo que en estas líneas sólo se incluye una breve descripción del programa. Puede encontrar un manual íntegro en <http://www.cis.upenn.edu/~bcpierce/unison/> o en el paquete SuSE unison.

Introducción a CVS

Campos de aplicación

El uso de CVS se recomienda para tareas de sincronización en el caso de ficheros individuales editados muy a menudo y cuyo formato es ASCII, texto fuente de programas o similar. Si bien es posible utilizar CVS para sincronizar datos en otros formatos (como por ejemplo JPEG), esto se traduce rápidamente en grandes cantidades de datos, ya que todas las versiones de un fichero se almacenan permanentemente en el servidor CVS. Además, en estos casos no se explota ni remotamente todo el potencial de CVS.

El uso de CVS para sincronizar datos sólo es posible cuando todas las estaciones de trabajo tienen acceso al mismo servidor.

A diferencia de CVS, el siguiente escenario también sería posible en el caso de unison:

$A > B > C > S$

A, B, C son ordenadores que pueden editar los datos en cuestión.

Configuración del servidor CVS

El "servidor" es el lugar donde están situados todos los ficheros válidos, es decir, especialmente la versión actual de cada fichero. Como servidor se puede utilizar una estación de trabajo de instalación fija. Se recomienda realizar periódicamente copias de seguridad de los datos del servidor CVS.

Una forma adecuada de configurar el servidor CVS consiste, por ejemplo, en autorizar a los usuarios el acceso vía SSH al mismo. De este modo, un ordenador de instalación fija pueda actuar como servidor.

Si el usuario es conocido en el servidor como tuxy el software CVS está instalado tanto en el servidor como en el cliente (ej. un notebook), en la parte del cliente hay que definir además las siguientes variables de entorno:

`CVS_RSH=ssh`

```
CVS_ROOT=tux@server:/serverdir
```

El comando `cvsv init` permite iniciar el servidor CVS desde la parte del cliente. Esta acción sólo debe realizarse una vez.

Finalmente hay que definir un nombre para la sincronización. Para ello, en un cliente se cambia al directorio que contiene exclusivamente datos administrados por CVS (también puede estar vacío). El nombre del directorio carece de importancia y en este ejemplo se llamará `synchome`. Para asignar a la sincronización el nombre de `synchome`, se ejecuta el comando:

```
cvsv import synchome tux tux_0
```

Nota: Muchos comandos de CVS requieren un comentario. Para ello, `cvsv` inicia un editor (aquél que ha sido definido en la variable de entorno `$EDITOR` o en su defecto `vi`). El inicio del editor se puede evitar introduciendo directamente el comentario en la línea de comandos, como por ejemplo en

```
cvsv import -m 'es una prueba' synchome tux tux_0
```

Manejo de CVS

A partir de este momento, el repositorio de la sincronización puede extraerse desde cualquier ordenador:

```
cvsv co synchome
```

Al ejecutar este comando se crea un nuevo subdirectorio `synchome` en el cliente. Si se han realizado modificaciones que quieren transmitirse al servidor, se cambia al directorio `synchome` (o a uno de sus subdirectorios) y se ejecuta el siguiente comando.

```
cvsv commit
```

Este comando transmite por defecto todos los ficheros (incluyendo subdirectorios) al servidor.

Si sólo se quieren transmitir determinados ficheros o directorios, éstos deben especificarse en el comando:

```
cvsv commit fichero1 ... directorio1 ...
```

Antes de ser transmitidos al servidor, los nuevos ficheros o directorios han de

declararse parte integrante de CVS:

```
cvcs add fichero1 ... directorio1 ...
```

y a continuación pueden enviarse al servidor

```
cvcs commit fichero1 ... directorio1 ...
```

Si se cambia el puesto de trabajo, debe en primer lugar extraerse el repositorio de la sincronización (véase arriba) si no se ha hecho ya en el transcurso de sesiones anteriores en ese mismo lugar de trabajo.

La sincronización con el servidor se inicia mediante el comando:

```
cvcs update
```

También es posible actualizar ficheros o directorios de manera selectiva:

```
cvcs update fichero1 ... directorio1 ...
```

Si se quieren ver las diferencias entre las versiones almacenadas en el servidor, se utiliza el comando

```
cvcs diff
```

o bien

```
cvcs diff fichero1 ... directorio1 ...
```

De manera alternativa, se puede utilizar el siguiente comando para mostrar los ficheros afectados por una actualización:

```
cvcs -nq update
```

En la actualización se utilizan entre otros, los siguientes símbolos indicadores de estado:

U la versión local ha sido actualizada

M la versión local ha sido modificada pero no actualizada

P la versión local ha sido parcheada. Es decir, CVS ha intentado fusionar la versión en el servidor CVS con la versión local

? este fichero no se encuentra en CVS

El estado **M** señala un conflicto que es necesario resolver. Para ello, se envía la copia local al servidor ("commit") o se elimina la copia local y se lleva a cabo una actualización, con lo que el fichero que falta se obtiene del servidor.

Información adicional

Las posibilidades de CVS son muy extensas y aquí sólo se han mencionado algunas de ellas. Puede encontrar más información en las siguientes direcciones:

<http://www.cvshome.org/>
<http://www.gnu.org/manual/>

Introducción a mailsync

Campos de aplicación

Básicamente, mailsync resulta adecuado para realizar tres tareas:

- sincronización de mensajes de correo electrónico archivados localmente con mensajes almacenados en un servidor
- migración de buzones a otro formato o a otro servidor
- comprobación de la integridad de un buzón o búsqueda de duplicados

Configuración y manejo

Mailsync distingue entre el buzón en sí (lo que se conoce como store) y el enlace entre dos buzones (que se denomina channel). Las definiciones de store y channel se encuentra en el fichero `~/.mailsync`. A continuación se mencionan algunos ejemplos de stores:

Una definición sencilla sería la siguiente:

```
store saved-messages {  
    pat      Mail/saved-messages  
    prefix   Mail/  
}
```

En las líneas superiores, `Mail/` es un subdirectorio del directorio personal de usuario que contiene carpetas con mensajes, entre ellas la carpeta `saved-messages`.

Si se ejecuta `mailsync` con

```
mailsync -m saved-messages
```

se mostrará un índice de todos los mensajes guardados en `saved-messages`. Si se define

```
store localdir {  
    pat      Mail/*  
    prefix   Mail/  
}
```

la ejecución de

```
mailsync -m localdir
```

produce una lista de todos los mensajes almacenados en las carpetas de Mail/.
El comando

```
mailsync localdir
```

produce una lista con los nombres de las carpetas. La definición de un store en un servidor IMAP sería por ejemplo:

```
store imapinbox {  
    server {mail.uni-hannover.de/user=gulliver}  
    ref    {mail.uni-hannover.de}  
    pat     INBOX  
}
```

El ejemplo superior sólo se refiere a la carpeta principal del servidor IMAP. Un store para una subcarpeta se definiría así:

```
store imapdir {  
    server {mail.uni-hannover.de/user=gulliver}  
    ref    {mail.uni-hannover.de}  
    pat     INBOX.*  
    prefix  INBOX.  
}
```

Si el servidor IMAP soporta conexiones cifradas, la definición del servidor ha de cambiarse a

```
server {mail.uni-hannover.de/ssl/user=gulliver}
```

o, en caso de que el certificado del servidor no se conozca, a

```
server {mail.uni-hannover.de/ssl/novalidate-cert/user=gulliver}
```

El prefijo se explicará más adelante.

Ahora es necesario conectar las carpetas de Mail/ con los subdirectorios del servidor IMAP:

```
channel carpeta localdir imapdir {  
    msinfo .mailsync.info  
}
```

Durante este proceso, mailsync registra en el fichero definido con `msinfo` qué mensajes han sido ya sincronizados.

La ejecución de

```
mailsync carpeta
```

produce como resultado lo siguiente:

- el patrón del buzón (`pat`) se amplía en ambas partes
- se elimina el prefijo (`prefix`) de los nombres de carpetas creados con este procedimiento
- las carpetas se sincronizan por pares (o son creadas en caso de no estar todavía disponibles)

Por lo tanto, la carpeta `INBOX.sent-mail` del servidor IMAP es sincronizada con la carpeta local `Mail/sent-mail` (suponiendo las definiciones anteriores). La sincronización entre las carpetas individuales se producen del siguiente modo:

- si un mensaje existe en ambas partes, no sucede nada
- si un mensaje falta en un lado y es nuevo (es decir, no está registrado en el fichero `msinfo`) será transmitido a esa parte
- si un mensaje existe sólo en una parte y es antiguo (ya está registrado en el fichero `msinfo`), será eliminado (ya que al parecer ya había existido en el otro lado y ha sido borrado)

Para obtener a priori una idea de qué mensajes serán transmitidos y cuáles serán borrados al realizar la sincronización, se puede activar mailsync con un `channel` y un `store` simultáneamente:

```
mailsync carpeta localdir
```

De esta forma se obtiene una lista de todos los mensajes que son nuevos localmente y otra lista de los mensajes que serían borrados en la parte del servidor IMAP si se realizase una sincronización.

De manera inversa, con

```
mailsync carpeta imapdir
```

se obtiene una lista con todos los mensajes nuevos en la parte del servidor y otra con los mensajes que serían borrados localmente si se realizase la sincronización.

Posibles problemas

En caso de pérdida de datos, el procedimiento más seguro consiste en borrar el fichero de registro "msinfo" correspondiente al canal. De esta forma, todos los mensajes que sólo existan en una parte se considerarán como nuevos y serán transmitidos con la siguiente sincronización.

En la sincronización se tienen en cuenta sólo los mensajes que tienen un message ID. Los mensajes que carezcan de éste serán ignorados, es decir, ni transmitidos ni eliminados. El message ID puede faltar debido a programas defectuosos en el proceso de entrega de correo o en el de creación de mensajes.

En algunos servidores IMAP, la carpeta principal se conoce con el nombre de INBOX y las subcarpetas con nombres arbitrarios (al contrario que en INBOX e INBOX.name). Esto provoca que en estos servidores IMAP no sea posible definir un patrón exclusivamente para las subcarpetas.

Después de la transmisión exitosa de mensajes a un servidor IMAP, los controladores para buzones (c-client) utilizados por mailsync colocan una bandera de estado especial. Esta bandera no permite a algunos programas de correo como mutt detectar el mensaje como nuevo. Para evitar la colocación de estas banderas de estado en mailsync, puede utilizar la opción `-n`.

Información adicional

Puede encontrar más información en el README incluido en el paquete mailsync en `/usr/share/doc/packages/mailsync/`.

El RFC 2076 "Common Internet Message Headers" también contiene información de gran interés.

Redes heterogéneas

Linux no sólo se puede comunicar con otros ordenadores Linux, sino también con máquinas Windows y Macintosh, así como con redes Novell. Este capítulo le muestra cómo puede configurar las correspondientes redes heterogéneas y qué debe tener en cuenta.

Samba	448
Netatalk	457
Emulación de Novell Netware con MARSNWE	464

Samba

Con la ayuda del programa Samba, del australiano Andrew Tridgell, un ordenador Unix puede convertirse en un servidor de archivos y de impresión para máquinas DOS, Windows u OS/2. Desde el comienzo de su desarrollo en 1991, Samba se ha convertido en un producto muy estable ocupando un sitio fijo en el mundo empresarial, donde se usa como complemento o incluso como reemplazo de los servidores Novell NetWare o Windows NT.

Samba es ya un producto muy completo y, por eso, aquí nos centramos exclusivamente en su funcionalidad. Sin embargo el software viene con una completa documentación digital, compuesta por un lado de páginas de manual – escriba `apropos samba` en la línea de comandos – y por otro de documentos y ejemplos que se instalaron en su sistema junto con Samba – en `/usr/share/doc/packages/samba`. Allí, en el subdirectorio `examples` también encontrará un ejemplo de configuración comentado `/smb.conf`. SuSE.

Samba usa el protocolo SMB (Server Message Block) que se basa en los servicios de NetBIOS. Por la insistencia de la empresa IBM, Microsoft publicó el protocolo para que otras empresas pudieran desarrollar software para conectar a una red con dominios de Microsoft. Como Samba usa el protocolo SMB sobre TCP/IP, en todos los clientes se debe instalar el protocolo TCP/IP. Le recomendamos utilizar TCP/IP de forma exclusiva.

NetBIOS

NetBIOS es una interfaz para programas de aplicación (ingl. *Application Program Interface, API*), que se diseñó para la comunicación entre ordenadores. Entre otros, ofrece un servicio de nombres (ingl. *name service*) mediante el cual los ordenadores se identifican entre sí. No existe ningún control centralizado para otorgar o controlar los nombres. Cada ordenador puede reservar en la red tantos nombres como quiera, mientras no se haya adelantado otra.

Se puede implementar la interfaz NetBIOS sobre diferentes arquitecturas de red. Hay una implementación que se encuentra relativamente “cerca” al hardware de red llamada NetBEUI. NetBEUI es lo que se denomina frecuentemente como NetBIOS.

Protocolos de red que se han implementado son NetBIOS son IPX (NetBIOS vía TCP/IP) de Novell y TCP/IP.

Los nombres de NetBIOS no tienen nada en común con aquellos asignados en el archivo `/etc/hosts` o por DNS – NetBIOS es un área de nombres completamente propio. Esto es válido también para los nombres que se asignan en la implementación de NetBIOS mediante TCP/IP. Sin embargo, para simplificar

la administración se recomienda usar, como mínimo para los servidores, nombres de NetBIOS equivalentes a los del DNS. Para un servidor Samba ésta es la opción por defecto.

Clientes

Todos los sistemas operativos ordinarios como Mac OS X, Windows y OS/2 soportan el protocolo SMB. Los ordenadores deben tener TCP/IP instalado. Samba proporciona también un cliente para las diversas versiones UNIX. En el caso de Linux, existe para SMB un módulo del kernel para el sistema de archivos que permite integrar recursos SMB a nivel del sistema en Linux.

Los servidores SMB ofrecen a los clientes espacio en disco en forma de "shares". Un share es un directorio en el servidor con todos los subdirectorios. Éste se exporta con un nombre determinado por medio del cual los clientes pueden acceder a él. El nombre del share es arbitrario, no hace falta que coincida con el nombre del directorio exportado. De la misma manera se asigna un nombre a una impresora exportada mediante el cual los clientes puedan acceder a ella.

Instalación y configuración del servidor

Si quiere utilizar Samba como servidor, instale el paquete `samba`. Los servicios necesarios para Samba se inician manualmente con el comando `rcnmb start && rcsmb start` y se paran con `rcsmb stop && rcnmb stop`.

El archivo de configuración central de Samba es `/etc/samba/smb.conf`. Éste puede dividirse en dos secciones lógicas: la sección `[global]` y la `[share]`. La primera sección sirve para las configuraciones globales y la segunda determina las autorizaciones de acceso a archivos e impresoras. Este procedimiento permite que algunos detalles de las autorizaciones de acceso sean distintos o bien fijarlos para todo el sistema en la sección `[globals]`, lo que se recomienda por motivos de claridad.

A continuación se explicarán algunos parámetros con más detalle,

Sección global en base a una configuración de muestra

Los siguientes parámetros de la sección `global` residen en su red para que su servidor Samba en una red Windows puede ser accesible desde otros sistemas vía SMB.

workgroup = TUX-NET Con esta línea, el servidor Samba asignará un grupo de trabajo. Para el funcionamiento, acomode TUX-NET al grupo de trabajo que tenga a su disposición o configure su cliente con el valor que se

encuentra aquí. En esta configuración su servidor Samba aparece con su nombre DNS en el grupo de trabajo elegido, siempre que no se haya cedido el nombre.

Si ya se ha adjudicado el nombre, puede establecer algo diferente del nombre DNS mediante `netbiosname=MINOMBRE`. Los detalles de este parámetro están disponible vía `man smb.conf`.

os level = 2 En función de este parámetro el servidor Samba decide si quiere convertirse en un LMB (ingl. *Local Master Browser*) para su grupo de trabajo. Se ha escogido un valor bajo en el ejemplo a propósito para que la red de Windows disponible no se vea perturbada por un servidor Samba mal configurado. Puede encontrar más detalles sobre este tema tan importante en los archivos `BROWSING.txt` y `BROWSING-Config.txt` que se encuentran en el subdirectorio `textdocs` de la documentación del paquete.

Si no hay en funcionamiento un servidor SMB — p. ej. Windows NT, 2000 Server — y el servidor Samba debe ordenar los nombres de los sistemas disponibles en la red local, aumente `os level` a un valor más alto (p. ej. 65), para conseguir convertirse en LMB.

Tenga mucho cuidado al modificar este valor, ya que puede perturbar el funcionamiento de una red Windows ya disponible. Hable con el administrador, pruebe los cambios primero en una red aislada o en momentos críticos.

wins support y wins server Si quiere integrar el servidor Samba en una red Windows ya disponible en la que existe un servidor WINS, debe activar el parámetro `wins server` eliminando el punto y coma, y acomodando la dirección IP a sus características.

Sus sistemas Windows funcionarán en subredes separadas si observa que *no* existe un servidor WINS en la red Windows y su servidor Samba debe convertirse en el servidor WINS. Para ello active la línea con `wins support = yes`. Compruebe que este parámetro se activa exclusivamente para un servidor Samba. Además no se debe activar `wins server` en este entorno.

Recursos compartidos

En los siguientes ejemplos se comparte por un lado la unidad de CD-ROM y por otro los directorios del usuario `homes` con los clientes SMB.

[cdrom]

```
;[cdrom]
;      comment = Linux CD-ROM
;      path = /media/cdrom
;      locking = No
```

Fichero 44: Acceso al CD-ROM

Para impedir el acceso libre a un CD-ROM por error, se han desactivado en este ejemplo todas las líneas correspondientes a este recurso compartido por medio de un signo de comentario (aquí punto y coma). Si desea autorizar el acceso a la unidad de CD-ROM por Samba, borre los signos de punto y coma en la primera columna.

- `[cdrom]` y `[comment]` La sección `[cdrom]` es el nombre del recurso compartido visible para el cliente SMB. Con `[comment]` se puede dar una descripción del recurso compartido al cliente.
- `path = /media/cdrom` Con `path` se exporta el directorio `/media/cdrom`.

Debido a una configuración intencionadamente restrictiva, este tipo de recursos compartidos sólo están disponibles para el usuario que se encuentre en el sistema. Si debe estar disponible para todo el mundo, añada otra línea `guest ok = yes`. Debido a las posibilidades de lectura que ofrece, se debe tener mucho cuidado con esta configuración y utilizarla solamente en ciertos recursos compartidos. Se ha de tener un cuidado especial en la sección `[global]`.

[homes]

El recurso compartido `[home]` tiene un significado especial: Si el usuario en cuestión dispone de una cuenta válida en el servidor de archivos y de un directorio personal en el mismo, es posible conectarse a este directorio mediante nombre y contraseña.

[homes]

```
comment = Home Directories
valid users = %S
browseable = No
read only = No
create mask = 0640
directory mask = 0750
```

Fichero 45: Recurso compartido homes

- **[homes]** Mientras no exista una autorización de acceso expresa con el nombre de autorización del usuario asociado, se creará una autorización de forma dinámica debido al recurso compartido **[homes]**. El nombre de este recurso compartido será idéntico al nombre de usuario.
- **valid users =%S%S** será reemplazada por el nombre concreto del recurso compartido tras haber realizado la conexión adecuadamente. Puesto que en el caso del recurso compartido **[homes]** éste siempre es idéntico al nombre de usuario, los usuarios autorizados se limitan al dueño del directorio de usuario. Esta es una posibilidad para permitir el acceso al dueño solamente.
- **browseable = No** Con esta configuración **[homes]** no será visible en la lista de recursos compartidos.
- **read only = No** En la configuración predeterminada, Samba deniega el permiso de escritura en los recursos compartidos exportables, **read only = Yes**. Si un directorio debe tener también permiso de escritura, asigne el valor **read only = No**, que equivale a **writable = Yes**.
- **create mask = 0640** Los sistemas no basados en MS Windows NT no conocen el concepto de permisos de acceso de Unix. Por lo tanto, al crear los archivos, no pueden establecer los permisos de acceso correspondientes.
El parámetro **create mask** establece los permisos de acceso que corresponden a los archivos. Esto sólo es válido para recursos compartidos en los que se pueda escribir. En concreto, al dueño se le permitirá leer y escribir, y a los componentes del grupo primario del usuario sólo la lectura. Tenga en cuenta que **valid users =%S** impide la lectura aún cuando el grupo esté autorizado. Para otorgar al grupo derechos de lectura y escritura, la línea **valid users =%S** ha de ser desactivada.

Niveles de seguridad

El protocolo SMB viene del mundo DOS y Windows y contempla los problemas de seguridad directamente. Todos los accesos a un share se protegen con una contraseña. SMB ofrece tres posibilidades para comprobar la autorización:

- **Share Level Security:** En este caso cada share tiene una contraseña fija. Cada persona que conoce la contraseña tiene acceso al share.
- **User Level Security:** Esta variante introduce el concepto de usuario SMB. Cada usuario tiene que darse de alta en el servidor con una contraseña

propia. Después de la autenticación, el servidor puede otorgar derechos de acceso a los distintos shares exportados en función del nombre de usuario.

- **Server Level Security:** Samba aparenta frente a los clientes trabajar en el "User Level Mode", pero en realidad pasa todas las peticiones de entrada a otro ordenador que se encarga de la autenticación. Esta configuración requiere de un parámetro adicional (`password server =`).

La decisión sobre el tipo de autenticación es algo que afecta a todo el servidor. No es posible exportar algunos shares de la configuración de un servidor en modalidad "Share Level Security" y otros en "User Level Security". No obstante, en un sistema puede operar un servidor Samba propio para cada dirección IP configurada.

El archivo `textdocs/security_level.txt` contiene más información al respecto. En el caso de un sistema con varios servidores, tenga en cuenta los parámetros `interfaces` y `bind interfaces only`.

Truco

Existe un programa denominado `swat` que permite administrar fácilmente el servidor samba, ya que ofrece una interfaz de web sencilla para configurarlo cómodamente. Dentro de un navegador introduzca `http://localhost:901` y entre al sistema como `root`. Hay que considerar que `swat` se activa también en los archivos `/etc/xinetd.d/samba` y `/etc/services`. Para ello debe modificar la línea `disable = no`. Puede obtener información adicional acerca de este programa en la página del manual de `swat` (`man swat`).

Truco

Samba como servidor de dominio

En redes con gran cantidad de clientes Windows, se prefiere que los usuarios sólo puedan acceder a los recursos con su nombre de usuario y una contraseña. Un servidor Samba puede realizar esta autenticación. En una red basada en Windows, un servidor de Windows-NT se encarga de esta tarea cuando está configurado como Primary Domain Controller (PDC). Para realizarlo con Samba es necesario introducir en la sección `[globals]` de `smb.conf` las entradas correspondientes como en el ejemplo 46.

```
[global]
workgroup = TUX-NET
domain logons = Yes
domain master = Yes
```

***Fichero 46:** Sección global en smb.conf*

Para usar contraseñas codificadas para la autenticación, como sucede de manera estándar en versiones mantenidas de MS Windows 9x, MS Windows NT 4.0 a partir del service pack 3 y todos los productos posteriores, hay que configurar el servidor Samba de tal forma que sepa manejarlas. Esto se realiza mediante la entrada `encrypt passwords = yes` dentro de la sección `[global]`. Además, las cuentas de los usuarios y las contraseñas se deben codificar en una forma que Windows entienda; se puede realizar mediante el comando `smbpasswd -a name`. Según el concepto de dominio de Windows NT, los propios ordenadores necesitan una cuenta de dominio que se genera mediante los siguientes comandos:

```
useradd nombre_ordenador\$
smbpasswd -a -m nombre_ordenador
```

***Fichero 47:** Creación de una cuenta de ordenador*

En el caso del comando `useradd` se ha añadido el símbolo del dólar mientras que el comando `smbpasswd` añade este carácter automáticamente al usar el parámetro `-m`.

En el ejemplo de configuración comentado se encuentran configuraciones que automatizan este trabajo.

```
add user script = /usr/sbin/useradd -g machines \
                 -c "NT Machine Account" -d \
                 /dev/null -s /bin/false%u$
```

***Fichero 48:** Creación automática de una cuenta de ordenador*

En el caso de la autenticación aquí elegida, todos los datos de usuario se guardan en `/etc/samba/smbpasswd`. Si quiere almacenar estos datos en un servidor LDAP, debe cambiar la variable `SAMBA_SAM` a `ldap` en YaST | Sistema | Editor para `/etc/sysconfig` | Servicios de red | Samba y a continuación activar el módulo samba de `SuSEconfig`.

Instalación de los clientes

Los clientes sólo pueden acceder al servidor Samba vía TCP/IP. Actualmente no es posible usar con Samba NetBEUI o NetBIOS sobre IPX.

Windows 95/98

Windows 95/98 trae el soporte de TCP/IP incorporado, pero al igual que Windows 3.11 no se instala con la configuración por defecto. Para la instalación de TCP/IP en un Windows ya instalado, se selecciona el icono de red en el panel de control y después 'Agregar...', 'Protocolo' TCP/IP de Microsoft. Después de reiniciar el ordenador Windows puede encontrar el servidor Samba en el entorno de red haciendo doble clic con el ratón sobre el icono correspondiente en el escritorio.

Truco

Para usar una impresora conectada al servidor Samba, se recomienda instalar en el cliente el driver general para impresoras PostScript o el usado para impresoras Postscript de Apple (se usan los drivers que vienen junto con la versión de Windows). Después se conecta con la cola de impresión de Linux que acepta PostScript como formato de entrada.

Truco

Optimización

`socket options` ofrece una posibilidad de optimización. La configuración predeterminada del ejemplo de configuración incluido está orientada a una red Ethernet local. Más detalles en página del manual de `smb.conf` (`man smb.conf`) en la sección `socket options` y en página del manual de `socket(7)` (`man socket(7)`). Más información en `textdocs/Speed.txt` y `textdocs/Speed2.txt`.

La configuración estándar en `/etc/samba/smb.conf` intenta proponer valores de amplio alcance orientándose a la configuración por defecto del equipo de Samba. Sin embargo, el ofrecer una configuración ya preparada resulta imposible desde el punto de vista de la configuración de red y de los nombres de grupos de trabajo. En el ejemplo de configuración comentado `examples/smb.conf` SuSE se encuentran indicaciones que le serán de ayuda para adaptarse a las circunstancias locales.

Truco

El equipo Samba incluye en `textdocs/DIAGNOSIS.txt` una introducción paso a paso para probar la configuración.

Truco

Netatalk

Con el paquete `netatalk` le permite implementar un potente servidor de archivos y de impresión para clientes Apple. Así, es posible acceder a datos del ordenador Linux desde la máquina Macintosh o bien imprimir en una impresora conectada.

Netatalk es un conjunto de programas Unix que se basan en el DDP (ingl. *Datagram Delivery Protocol*) del kernel e implementan la familia de protocolos de AppleTalk (ADSP, ATP, ASP, RTMP, NBP, ZIP, AEP y PAP).

En principio, AppleTalk es el equivalente del ampliado TCP (Transmission Control Protocol). Muchos de los servicios TCP/IP, p. ej. la resolución de nombres y la sincronización horaria, equivalen a los de AppleTalk. Así por ejemplo, en vez del comando `ping` (ICMP ECHO_REQUEST, Internet Control Message Protocol) utiliza `aecho` (AEP, AppleTalk Echo Protocol).

Los siguientes tres daemons se inician normalmente en el servidor:

- El `atalkd` ("Administrador de red de AppleTalk"), que se corresponde por así decirlo con `ifconfig` y `routed`;
- El `afpd` (AppleTalk Filing Protocol Daemon), que proporciona una interfaz de sistema de datos Unix para clientes de Macintosh.
- El `pppd` (Printer Access Protocol Daemon), que incorpora la impresora a la red (de AppleTalk).

En el servidor, puede exportar al mismo tiempo directorios a través de Samba (para clientes de Windows, ver el capítulo anterior) y de NFS (ver [13](#) en la página [382](#)), lo cual resulta muy útil en entornos de red heterogéneos. La protección de datos y la administración de los derechos de acceso se pueden realizar centralmente en el servidor Linux.

Al utilizar el programa Netatalk tenga en cuenta lo siguiente:

- Debido a las restricciones de los clientes de Macintosh, las contraseñas de los usuarios en el servidor han de tener 8 caracteres como máximo.
- Los clientes de Macintosh no tienen acceso a archivos de Unix cuyo nombre tenga más de 31 caracteres.
- Los nombres de archivo no deben incluir dos puntos (':'), porque este signo funciona como separador en los nombres de ruta de MacOS.

Configuración del servidor de archivos

En la configuración estándar, "Netatalk" es ya un servidor de archivos completamente funcional para todos los usuarios dados de alta en el sistema Linux. Para usar otras funciones adicionales, es necesario realizar algunos ajustes en los archivos de configuración que se encuentran en el directorio `/etc/netatalk`.

Todos los archivos de configuración son archivos de texto. Las líneas que comienzan con el símbolo `'#'` y las vacías se ignoran ya que se consideran comentarios.

Los distintos servicios (impresora, Appletalk Broadcast, Appletalk a través de TCP/IP, servidor de tiempo) se activan a través del archivo `/etc/netatalk/netatalk.conf`:

```
ATALKD_RUN=yes
PAPD_RUN=yes
AFPD_RUN=yes
TIMELORD_RUN=no
```

Configurar la red – `atalkd.conf`

El archivo `/etc/atalk/atalkd.conf` define las interfaces a través de las cuales se ofrecen los servicios de AppleTalk. Esta interfaz es a menudo `eth0` y suele ser suficiente con introducir:

```
eth0
```

como valor único (es el caso de este ejemplo). Aquí puede añadir más interfaces, p. ej. si utiliza más de una tarjeta de red simultáneamente. Cuando arranca el servidor, éste busca en la red zonas y servidores que ya estén disponibles, tras lo cual modifica las líneas correspondientes introduciendo las direcciones de red de AppleTalk configuradas. Al final del archivo encuentra entonces una línea semejante a

```
eth0 -phase 2 -net 0-65534 -addr 65280.57
```

Si quiere realizar configuraciones más complejas, puede encontrar varios ejemplos en el archivo de configuración. Puede obtener también documentación sobre opciones adicionales en la página del manual de `afpd`.

Definir el servidor de archivos – `afpd.conf`

En el archivo `afpd.conf` se define cómo ha de aparecer el servidor de archivos para los clientes Apple en la ‘Selección’. Como el resto de archivos de configuración, éste también incluye comentarios detallados que le explicarán las diversas opciones.

Si no se modifica nada aquí, arranca el servidor por defecto el cual se mostrará en el ‘Selección’ con el nombre del host. Por lo tanto, no es necesario introducir necesariamente algo en este apartado. En este archivo además se puede definir otro servidor con un nombre diferente p. ej. definir un servidor de “invitados” que permita a los “huéspedes” dejar archivos en él.

```
"Guest server" -uamlist uams_guest.so
```

O puede definir un servidor que no permita la entrada a huéspedes, sino sólo a usuarios que ya existan en el sistema Linux:

```
"Font server" -uamlist uams_clrtxt.so,uams_dhx.so
```

Este proceso quedará guardado a través de la opción `uamlist` seguido de una lista de los módulos de autenticación que deben emplearse separados por comas. Por defecto, todos los procesos están activos.

Por regla general, un servidor AppleShare no sólo ofrece sus servicios a través de AppleTalk, sino también “encapsulado” a través de TCP/IP. El puerto por defecto es 548. Si quiere disponer de más servidores AppleShare (en el mismo ordenador) que también funcionen a través de TCP/IP, debe asignar puertos dedicados. El proporcionar los servicios vía TCP/IP permite acceder al servidor a través de redes que no sean AppleTalk, como por ejemplo Internet.

La sintaxis sería p. ej.:

```
"Font server" -uamlist uams_clrtxt.so,uams_dhx.so -port 12000
```

Aquí, el servidor AppleShare que aparece en la red con el nombre “font server”, no permite ningún acceso a los huéspedes y el puerto es 12 000. Por lo tanto, también se puede acceder a él a través de un router TCP/IP.

Los directorios del servidor que el servidor AppleShare correspondiente podrá a

En el archivo `AppleVolumes.default` quedan definidos los directorios del servidor que el servidor AppleShare correspondiente proporcionará en forma de “volúmenes de red”. Mediante la opción `-defaultvol` puede definir otro archivo para un único servidor AppleShare en el que se indiquen instrucciones diferentes, p. ej. (en una línea):

```
"Guest server" -uamlist uams_guest.so -defaultvol  
/etc/netatalk/AppleVolumes.guest
```

En el archivo `afpd.conf` se explican otras opciones.

Directorios y permisos de acceso – AppleVolumes.default

Aquí se determinan los directorios que deben ser exportados. Los permisos de acceso quedan establecidos mediante los derechos de usuario y grupo normales en Unix.

Esto se configura en el archivo `AppleVolumes.default`.

Atención

Aquí ha cambiado parcialmente la sintaxis. Téngalo en cuenta si está actualizando desde una versión antigua, p. ej. en vez de `access=`, ahora es `allow`: (un síntoma característico sería si en los clientes Mac con AppleTalk se mostrasen las opciones en vez de la descripción de una unidad determinada.) Puesto que con la actualización han aparecido nuevos archivos con la extensión `.rpmnew`, puede que, en determinadas circunstancias y debido al cambio de sintaxis, la antigua configuración no funcione.

Le recomendamos hacer una copia de seguridad de los archivos de configuración, con el fin de incorporar la configuración anterior a los nuevos archivos y renombrarlos. De este modo puede aprovecharse de los detallados comentarios que se incluyen ahora y que le explicarán las diversas opciones posibles en los archivos de configuración.

Atención

Es posible que existan archivos adicionales junto a `AppleVolumes.default`, p. ej. `AppleVolumes.guest`, utilizados por determinados servidores (en el archivo `afpd.conf` se usa la opción `-defaultvol` – ver apartado anterior).

La sintaxis es bastante sencilla:

```
/usr/local/psfonts "PostScript Fonts"
```

significa que el directorio Linux `/usr/local/psfonts` que se encuentra en el directorio root, se comparte como volumen AppleShare con el nombre "PostScript Fonts".

Las distintas opciones se añaden a la línea separadas por espacios en blanco. Una opción muy útil es la de restricción de accesos.


```
/usr/local/psfonts "PostScript Fonts" allow:Usuario1,@grupo0
```

limita el acceso al volumen "PostScript Fonts" al usuario "Usuario1" y a todos los miembros del grupo "grupo0", los cuales ya deberán ser conocidos por el servidor. De forma análoga se puede excluir explícitamente a un usuario con `deny:Usuario2`.

Tenga en cuenta que estas limitaciones tienen validez para el acceso vía AppleTalk, pero no tienen nada que ver con los permisos de acceso de un usuario al hacer un login en el servidor.

Netatalk coloca en el Resource-Fork de archivos típico de Mac el directorio `.AppleDouble`. Con la opción `noadouble` puede determinar que estos directorios sólo sean creados cuando realmente se necesiten. La sintaxis es:

```
/usr/local/guests "Guests" options:noadouble
```

Puede encontrar explicaciones más detalladas de las distintas opciones en el archivo en cuestión.

Por lo demás: En los archivos de configuración puede encontrar un pequeño e inocente signo ('~'). Este signo simboliza el directorio raíz de cada usuario en el servidor. Con él, todos los usuarios pueden compartir su directorio raíz automáticamente, sin necesidad de incluirlos aquí de forma explícita. El archivo de ejemplo que se encuentra instalado incluye este signo, puesto que Netatalk ya proporciona por defecto el directorio raíz si Vd. no modifica nada en el archivo.

Además, el `afpd` busca en el directorio raíz de un usuario que se ha dado de alta los archivos `AppleVolumes` o `.AppleVolumes`. Las entradas de estos archivos complementan a las de los archivos del servidor `AppleVolumes.system` y `AppleVolumes.default` para permitir la asignación de más "type/creator" individuales y acceder a sistemas de archivos. Estas entradas son complementos y no autorizan ningún acceso que no se permita a través del servidor.

El archivo `netatalk.pamd` sirve para la autenticación con PAM (Pluggable Authentication Modules), lo cual no es relevante en este capítulo.

Asignación de archivos – `AppleVolumes.system`

El archivo `AppleVolumes.system` establece también la asignación de tipo (Type) y creador (Creator) a las terminaciones de los archivos. Algunas asignaciones estándar ya están predefinidas. Si un archivo aparece con un icono genérico en blanco es porque aún no se ha realizado ninguna asignación. En caso de problemas al abrir un archivo de texto de otro sistema en Mac o viceversa, aquí puede controlar las entradas.

Configuración del servidor de impresión

Mediante el archivo `papd.conf` se puede ofrecer un servicio del tipo "Apple Laserwriter". Esta impresora ya debe funcionar localmente mediante `lpd` (capítulo *Funcionamiento de la impresora* en la página 125). El primer paso ha finalizado cuando se puede imprimir localmente usando el comando `lpr archivo.txt`.

No debe añadir nada al `papd.conf` si se ha configurado una impresora local en Linux, puesto que los trabajos de impresión se envían directamente al daemon de impresión `lpd`. La impresora se presenta en la red AppleTalk como "Laserwriter". Pero también puede dar de alta una impresora de la siguiente forma:

```
impresora_oficina3:pr=lp:pd=/etc/netatalk/kyocera.ppd
```

Con esta configuración aparece en la selección una impresora denominada `impresora_oficina3`. El fabricante de la misma suministra normalmente el archivo de descripción correspondiente. En caso de no disponer de él, se puede usar en su lugar el archivo `Laserwriter` de la carpeta 'Extensiones de sistema' pero con la desventaja de no poder utilizar todas las funciones de la impresora.

Arrancar el servidor

El servidor arranca mediante el script de inicio, "Init-Script", o manualmente con `rcatalk start`. El script de inicio se encuentra en `/etc/init.d/atalk`. El script realiza el arranque en segundo plano; dura más o menos un minuto hasta que las interfaces de AppleTalk se configuran y están disponibles. Puede comprobar si el arranque ya ha sido realizado pidiendo un informe de la situación (si el OK aparece tres veces, el proceso ha sido completado):

```
tierra:~ # rcatalk status
```

```
"Checking for service atalk:OKOKOK"
```

Ahora diríjase a un ordenador Mac que funcione con Mac OS. Compruebe que AppleTalk está activado, escoja 'Filesharing', haga doble clic en 'Appleshare' y verá el nombre del servidor en la ventana que aparece. Haga doble clic en el nombre y regístrese. Escoja la unidad y – voilà – ahí se encuentra su unidad de red con Mac OS.

Para conectarse con servidores que sólo funcionan con TCP y no con DDP, diríjase a 'Selección', pulse 'Dirección IP del servidor' e introduzca la dirección IP correspondiente, de ser necesario, seguida de dos puntos y el número de puerto.

Información adicional

Para sacar el máximo provecho de todas las posibilidades que le ofrece el paquete `netatalk`, le recomendamos que consulte las páginas man correspondientes que encontrará con el comando: `rpm -qd netatalk` Otra indicación: El archivo `/etc/netatalk/netatalk.conf` no se utiliza en nuestra versión de `netatalk`, por lo tanto puede pasarlo por alto.

Algunas URLs de utilidad:

- <http://netatalk.sourceforge.net/>
- <http://www.umich.edu/~rsug/netatalk/>
- <http://www.anders.com/projects/netatalk/>
- <http://cgi.zettabyte.net/fom-serve/netatalk/cache/1.html>

¿Puedo acceder a una unidad AppleShare con Linux? La respuesta más sincera es: Mejor no lo intente porque el paquete correspondiente se encuentra todavía en fase muy experimental. Quien no tenga miedo a experimentar puede encontrarlo en: <http://www.panix.com/~dfoster/afpfs/>

Emulación de Novell Netware con MARSNWE

Es relativamente fácil reemplazar un servidor de ficheros y de impresión de Novell-Netware 2.2 o 3.11 mediante el emulador de Netware MARSNWE. Éste también permite que funcione como router IPX. Por otra parte, no es capaz de emular las funcionalidades adicionales de versiones más recientes como p. ej. los servicios de directorio NDS (ingl. *Netware Directoy Services*). Las estaciones de trabajo a base de DOS o Windows que ya están configuradas para acceder a un servidor Netware 2.2/3.11/3.12 casi no necesitan modificaciones para trabajar con el servidor Linux y la emulación MARSNWE. La administración del servidor se realiza directamente desde Linux, ya que los programas de Novell para la administración no funcionarían completamente y se tuviera que considerar la licencia de los mismos.

Iniciar el emulador de netware MARSNWE

En SuSE Linux se puede iniciar y probar MARSNWE directamente después de la instalación ya que está correctamente preconfigurado. El soporte de IPX que necesita el kernel se realiza mediante un módulo que se carga automáticamente por el script de inicio. MARSNWE se encarga de configurar automáticamente la interfaz IPX, tomando como referencia los valores del número de red y del protocolo a utilizar desde el fichero de configuración `/etc/nwserv.conf`. El comando para inicializar MARSNWE es `rcnwe start`. El mensaje `done` en la derecha de la pantalla indica el inicio correcto del programa.

`rcnwe status` es el comando para comprobar el estado de ejecución del emulador de Netware; para terminarlo se utiliza `rcnwe stop`.

El fichero de configuración `/etc/nwserv.conf`

Las opciones de configuración se agrupan en secciones ("Sections") numeradas. Cada línea de configuración comienza con el número de la sección correspondiente. Las secciones interesantes son aquellas con números de 1 hasta 22. Normalmente las siguientes secciones alcanzan para la configuración:

- 1 Volumen es de Netware
- 2 Nombre del servidor
- 4 Red/Dispositivos IPX

13 Nombres de usuarios**21** Colas de impresión

Hay que reiniciar MARSNWE con el comando `rcnwe restart` después de cualquier cambio de la configuración.

Las opciones de configuración en detalle:

Volúmenes (Sección 1):

```
1      SYS      /usr/local/nwe/SYS/      kt      711 600
```

Sección para definir los volúmenes a exportar. Cada línea comienza con el número de la sección (en este caso 1) seguido del nombre de volumen y de la trayectoria del directorio en el servidor. Se puede indicar varias opciones adicionales, representadas por letras tal como un "UMASK" para la creación de directorios y de ficheros. En caso de no especificar ningún "UMASK" se utiliza el valor por defecto de la sección 9. El volumen para SYS ya está configurado. En cuanto a las opciones se recomienda utilizar k para evitar problemas con mayúsculas y minúsculas en los nombres de ficheros. Activando la opción todos los nombres de ficheros se convierten a minúsculas.

Nombre del servidor (Sección 2):

```
2      MARS
```

Este parámetro es opcional; por defecto se utiliza el nombre del host.

Número de la red interna (Sección 3):

```
3      auto
```

Mediante el parámetro `auto` el número de red interno se genera a base de la dirección MAC de la tarjeta de red. Normalmente se ha de mantener el parámetro en `auto`.

Configuración IPX (Sección 4):

```
4      0x0      *      AUTO      1
4      0x22     eth0     ethernet_ii  1
```

En esta sección se puede indicar el número de red de netware, la interfaz de red y el protocolo que se debe utilizar. En el primer ejemplo la configuración es totalmente automática mientras que en el segundo caso se asigna el número de red 0x22 a la tarjeta de red eth0 con el protocolo Ethernet - II. Los paquetes IPX se rutean entre varias tarjetas que estén dadas de alta con diferentes números de red.

Modo de creación (Sección 9):

```
9      0751      0640
```

Definición de los permisos estándar para la creación de directorios y ficheros.

UID y GID con derechos mínimos (Sección 10, 11):

```
10     65534
```

```
11     65534
```

Número de identificación (ID) de grupo y de usuario para usuarios no registrados; en este caso nogroup y nobody.

Login de supervisor (Section 12):

```
12     SUPERVISOR      root
```

El supervisor se representa por el usuario root.

Logins de usuarios (Sección 13):

```
13     LINUX           linux
```

En este apartado se realiza la asignación entre usuarios de Netware y los usuarios de Linux. Como opción se puede indicar una contraseña fija.

Proyección automática de usuarios (Sección 15):

```
15     0              top-secret
```

Para hacer de los "logins" de Linux automáticamente logins de Netware hay que reemplazar 0 por 1. En este caso la contraseña es "top-secret".

Colas de impresión (Sección 21):

21 LP - lpr -

El primer parámetro (LP) es el nombre de la impresora Netware, como segundo parámetro se puede indicar el directorio temporal de impresión (spooling) y el tercero es el comando de impresión.

Servidor de impresión (Sección 22):

22 PS_NWE LP_PS 1

En esta línea se pueden configurar las impresoras a las que se acceden mediante pserver del paquete ncpfs.

Administración de servidores Netware

El paquete ncpfs es una recopilación de utilidades para la administración de servidores Netware 2.2/3.11 desde Linux. Estas sirven también para montar volúmenes de Netware o administrar impresoras. Hay que activar IPX y la emulación "Bindery" para acceder a servidores Netware a partir de la versión 4.

Existen las siguientes utilidades, cuyas funcionalidades se detallan en las páginas de manual de las mismas:

nwmsg	ncopy	ncpmount	ncpumount
nprint	nsend	nwauth	nwbocreate
nwbols	nwboprops	nwborm	nwbpadd
nwbpcrcreate	nwbprpm	nwbpset	nwbpvalues
nwdir	nwdpvalues	nwfscrtl	nwfinfo
nwfstime	nwgrant	nwpasswd	nwpurge
nwrevoke	nwrights	nwsfind	nwtrustee
nwtrustee2	nwuserlist	nwvolinfo	pqlist
pqrm	pqstat	pserver	slist

Un comando muy importante es **ncpmount** que sirve para montar volúmenes de un servidor de Netware bajo Linux y su homólogo **ncpumount** para desmontar el volumen nuevamente.

El paquete ncpfs contiene también herramientas para la configuración del protocolo IPX y para "routing" bajo IPX.

```
ipx_cmd  
ipx_configure  
ipx_interface  
ipx_internal_net  
ipx_route
```

`ipx_configure` o `ipx_interface` son las utilidades para la configuración de IPX de la tarjeta de red. Al iniciar MARSNWE, éste se encarga automáticamente de la configuración.

Router de IPX mediante ipxrip

Una alternativa para convertir un ordenador con Linux en un enrutador de IPX es el paquete `ipxrip`. Normalmente no se necesita debido a que MARSNWE o las herramientas del paquete `ncpfs` ya son capaces de configurar un enrutador de IPX.

Internet

Se puede escribir mucho sobre el tema de Internet, pero en el contexto de este manual nos limitaremos a dos temas principales: la configuración manual de una conexión ADSL – en caso de que surjan problemas en la configuración con VdST– y la configuración del proxy squid.

smppppd como asistente para la conexión telefónica	470
Configuración de una conexión ADSL	472
Servidor proxy: Squid	474

smpppd como asistente para la conexión telefónica

Componentes del programa para la conexión a Internet vía telefónica

La mayoría de los usuarios particulares no tiene una conexión fija a Internet, sino que se conecta vía telefónica cada vez que lo necesita. Dependiendo del tipo de conexión (RDSI o ADSL), los programas `ippd` o `pppd` se encargan de controlar esta conexión. En principio basta con iniciar estos programas correctamente para poder estar en línea.

Si se dispone de tarifa plana y la conexión no supone costes adicionales, es suficiente con iniciar el daemon de la manera adecuada. No obstante, a veces es deseable poder controlar mejor la conexión telefónica, ya sea mediante un applet de KDE o una interfaz de línea de comandos. Además, la pasarela a Internet no es siempre el propio ordenador de trabajo, por lo que resulta conveniente regular la conexión telefónica en un ordenador accesible en red.

Aquí es donde interviene el programa `smpppd`. Éste facilita a los programas de ayuda una interfaz uniforme que funciona en dos direcciones. Por un lado programa la herramienta necesaria `pppd` o `ippd` y regula su funcionamiento durante el marcado. Por el otro, proporciona a los programas de usuario diversos proveedores y transmite información sobre el estado actual de la conexión. Debido a que `smpppd` también puede controlarse en red, resulta muy adecuado para dirigir la conexión a Internet desde una estación de trabajo en la subred privada.

La configuración de smpppd

YaST asume automáticamente la configuración de las conexiones proporcionadas por `smpppd`. Los programas de marcado `kinternet` y `cinternet` están también preconfigurados. Sólo tendrá que configurar manualmente funciones adicionales de `smpppd`, como por ejemplo el manejo de forma remota.

El fichero de configuración de `smpppd` se encuentra en `/etc/smpppd.conf`. Está configurado de tal forma que no permite el manejo remoto por defecto. Las opciones más interesantes de este fichero de configuración son:

open-inet-socket = <yes|no> Si se desea controlar `smpppd` a través de la red, esta opción ha de tener el valor `yes`. El puerto en el que `smpppd` "escucha" es 3185. Si asigna el valor `yes` a este parámetro, los parámetros

`bind-address`, `host-range` y `password` han de configurarse en consecuencia.

`bind-address = <ip>` Si un ordenador dispone de varias direcciones IP, esta opción permite definir sobre qué dirección IP acepta conexiones `smpppd`.

`host-range = <min ip> <max ip>` El parámetro `host-range` puede utilizarse para definir una sección de red. El acceso a `smpppd` se permitirá sólo a los ordenadores cuyas direcciones IP estén dentro de esta sección; el resto de ordenadores será rechazado.

`password = <password>` Mediante la asignación de una contraseña es posible restringir los clientes sólo a ordenadores autorizados. Debido a que la contraseña está en texto plano, no hay que sobrevalorar su valor como medida de seguridad. Si no se define ninguna contraseña, todos los clientes pueden acceder a `smpppd`.

Puede encontrar más información sobre `smpppd` en página del manual de `smpppd` (`man 8 smpppd`) y página del manual de `smpppd.conf` (`man 5 smpppd.conf`).

Preparación de `kinernet` y `cinternet` para el uso remoto

Los programas `kinernet` y `cinternet` no sólo pueden utilizarse localmente, sino también controlar un `smpppd` remoto. `cinternet` es el equivalente en la línea de comandos al programa gráfico `kinernet`. Para preparar ambas herramientas para su uso con un `smpppd` remoto, debe editar el fichero de configuración `/etc/smpppd-c.conf` de forma manual o con `kinernet`. Este fichero sólo reconoce tres opciones:

`server = <server>` Aquí se puede especificar el servidor sobre el que funciona `smpppd`. Si el servidor es además la pasarela predeterminada del ordenador, basta con asignar el valor `yes` a `gateway-fallback`.

`gateway-fallback = <yes|no>` Si no se ha indicado ningún servidor o no funciona ninguno localmente, se puede intentar acceder a `smpppd` a través de la pasarela predeterminada. Esta opción está activada por defecto.

`password = <password>` Introduzca aquí la contraseña elegida también para `smpppd`.

Si `smpppd` se está ejecutando, puede intentar acceder a `smpppd` mediante el comando `cinternet --verbose --interface-list`.

Si se presentan dificultades, puede consultar página del manual de `smpppd-c.conf` (man 5 `smpppd-c.conf`) y página del manual de `cinternet` (man 8 `cinternet`).

Configuración de una conexión ADSL

Atención

El procedimiento expuesto en este capítulo se basa en la implementación de la tecnología xDSL en Alemania. Según el país y la compañía es posible que se utilicen tecnologías diferentes, con lo cual, la configuración local en su país podría ser diferente.

Atención

Configuración estándar

Actualmente SuSE Linux soporta aquellos accesos xDSL que trabajan con el protocolo Point-to-Point-over-Ethernet (PPPoE). Es el protocolo que emplean todos los proveedores grandes. Si no está seguro de qué protocolo usa su proveedor, éste seguramente le puede facilitar dicha información.

1. Los paquetes `ppp` y `smpppd` deben estar instalados; use YaST para instalarlos.
2. Configure su tarjeta red con YaST. No seleccione `dhcp`, sino especifique una dirección IP estática, p. ej.: `192.168.2.22`.
3. Los parámetros que se modifican con el módulo DSL de YaST se guardan en el fichero `/etc/sysconfig/network/providers/provider0`. Adicionalmente existen ficheros de configuración para `smpppd`, el Daemon-Meta-PPP de SuSE y sus frontales `kinternet` y `cinternet`. Tenga en cuenta la página de manual `refman smpppd`.
4. Si es necesario active la red con el comando `rcnetwork start` y a continuación el daemon `smpppd` con `rcsmpppd start`.
5. Con los comandos `cinternet -start` y `cinternet -stop` puede establecer o interrumpir una conexión en un sistema sin entorno gráfico. Si trabaja en un entorno gráfico, puede utilizar para ello el programa `kinternet`, el cual arranca automáticamente en KDE si ha configurado DSL

con YaST. Pulse sobre el icono de la rueda dentada en la barra de botones para establecer una conexión. Seleccione 'Comunicación/Internet' → 'Internet Tools' → 'kinternet'. Ahora aparece el símbolo de un enchufe en la barra de botones. Pulsando sobre él, la conexión se establece y un segundo clic cierra la conexión.

Conexión ADSL vía "Dial-on-Demand"

Dial-on-Demand o conexión bajo demanda, significa que la conexión se establece justo en el momento en que un usuario accede a Internet, p. ej. cuando selecciona una página web en el navegador o manda un E-Mail. Después de un tiempo determinado sin tráfico de red, la conexión se corta. Debido a que el establecimiento de la conexión por parte del protocolo PPPoE de ADSL es muy rápido, se tiene la impresión de que la conexión fuera continua.

Esta forma de conexión sólo se recomienda si tiene tarifa plana. De no ser así, es decir, si el proveedor le cobra por el tiempo de conexión, es importante vigilar que no exista ningún proceso que provoque una conexión periódica (p. ej. un cronjob) ya que los gastos podrían aumentar de forma considerable.

Hay algunas objeciones contra una conexión continua a Internet, incluso cuando la modalidad de acceso es la tarifa plana:

- La mayoría de los proveedores cortan la conexión después de un cierto tiempo.
- Una conexión continua es un cierto despilfarro de recursos (p. ej. de las direcciones IP).
- La conexión continua es sobre todo un gran riesgo de seguridad, ya que el atacante tiene tiempo para averiguar sistemáticamente posibles puntos débiles del sistema. Es mucho más difícil atacar un sistema que solo conecta a Internet bajo demanda y que obtiene cada vez una dirección IP diferente.

Es posible activar la conexión bajo demanda (dial on demand) con YaST (ver el manual del usuario) o configurándolo manualmente. En el fichero `/etc/sysconfig/network/providers/provider0` fije el parámetro `DEMAND=` a "yes" y defina el período de inactividad (ingl. *idle time*) con la variable: `IDLETIME="60"`.

De esta forma una conexión en la que no existe ninguna actividad se corta después de 60 segundos.

Para la configuración de gateways DSL para redes privadas, le recomendamos el siguiente artículo de nuestra base de datos de soporte: <http://sdb.suse.de/es/sdb/html/masq80.html>

Servidor proxy: Squid

El caché proxy por excelencia para plataformas Linux/UNIX es Squid, del que veremos cómo realizar su configuración, qué especificaciones requerirá el sistema donde lo vayamos a instalar, cómo llevar a cabo la configuración de un servidor proxy transparente y, finalmente, cómo obtener estadísticas sobre el uso del caché con la ayuda de programas como Calamaris y cachemgr o cómo utilizar la aplicación squidGuard para realizar filtrado de páginas web.

¿Qué es un caché proxy?

Squid se comporta como un caché proxy: esto es, actúa como un agente que recibe peticiones de clientes (en este caso navegadores web) y pasa estas peticiones al proveedor de servicios apropiado. Cuando los datos llegan de nuevo al agente, éste almacena una copia de los datos en un caché de disco.

Las ventajas de este sistema aparecen cuando varios clientes intentan acceder a los mismos datos: ya no hará falta ir a buscarlos otra vez a Internet, sino que se servirán directamente desde el caché de disco. De esta forma, los usuarios se benefician de un ahorro importante en el ancho de banda y en el tiempo de descarga.

Truco

Squid ofrece ventajas como la posibilidad de intercomunicar jerarquías de servidores proxys para repartir la carga entre ellos o establecer estrictas reglas de control de acceso para los clientes de las redes que quieran acceder al proxy. Además, con la ayuda de otras aplicaciones es posible controlar el acceso a determinadas páginas web u obtener estadísticas sobre cuáles son las webs más visitadas, con qué frecuencia los usuarios se conectan, etc.

Truco

Squid no es un proxy genérico. Actúa como proxy entre conexiones vía HTTP y soporta también los protocolos FTP, Gopher, SSL y WAIS, pero no soporta otros protocolos de Internet como por ejemplo Real Audio, News o videoconferencia. Squid sólo soporta el protocolo UDP para realizar comunicaciones entre diferentes cachés, con lo que muchos programas multimedia quedarán igualmente excluidos.

Información general sobre cachés proxy

Squid y seguridad

También es posible emplear Squid junto con un cortafuegos para proteger una red interna del exterior mediante un caché proxy. Exceptuando a Squid, el cortafuego impide a todos los clientes establecer conexiones a servicios externos, forzando a que sea el proxy quien establezca todas las comunicaciones con la World Wide Web.

Si la configuración del cortafuegos incluye un DMZ, es allí donde aplicaremos el servidor proxy. En ese caso, es importante que todos los ordenadores de la DMZ envíen sus archivos de registro (o logfiles) a ordenadores dentro de la red segura.

En el apartado [Configuración de un proxy transparente](#) en la página 485 se describe un método de implementar un proxy "transparente".

Cachés multinivel

Es posible configurar varios proxys para que cooperen intercambiando objetos entre ellos. De esta forma se reduce la carga total del sistema y se aumenta la probabilidad de que el objeto se encuentre ya en la red local. Es posible configurar incluso jerarquías de cachés, de forma que se pueda pedir páginas a cachés del mismo nivel o enviar peticiones a otros proxys de jerarquía más alta para que pidan las páginas a otros cachés existentes en la red o las obtengan directamente de la fuente.

Elegir una buena topología para los cachés es muy importante para no acabar creando más tráfico del que ya había en la red antes de instalar los cachés. Por ejemplo, para una red local muy extensa puede configurarse un servidor proxy para cada subred y conectar éstos a un proxy "padre" que, por ejemplo, esté a su vez conectado al caché proxy del ISP.

Toda esta comunicación se lleva a cabo mediante el protocolo ICP (Internet Cache Protocol) basado en UDP. Las transferencias de datos entre la mayoría de cachés se realizan mediante HTTP, protocolo basado en TCP.

Para encontrar el servidor más apropiado desde el que obtener un objeto, un caché envía una petición ICP a sus proxys vecinos. Éstos le enviarán respuestas ICP con código HIT, si el objeto se encuentra efectivamente allí, o bien MISS en caso contrario. En caso que haya varios HIT, el proxy se decidirá por un servidor en especial en función de factores como la velocidad de respuesta o la proximidad, entre otros. Si las respuestas de los proxys vecinos no son satisfactorias, la petición se realizará al caché principal.

Truco

Para evitar duplicaciones de los objetos en varios cachés en la red se utilizan otros protocolos ICP como CARP (Cache Array Routing Protocol) o HTCP (Hyper-Text Cache Protocol). Cuantos más objetos tengamos en la red, mayor será la posibilidad que esté el que buscamos.

Truco

Objetos cacheados en Internet

No todos los objetos disponibles en la red son estáticos. Existen páginas generadas dinámicamente por CGIs, contadores de visitantes o bien documentos que incluyen SSL para codificar el contenido y hacerlo más seguro. Por esos motivos se considera este tipo de objetos como no cacheables, ya que cada vez que se accede a ellos ya han cambiado.

Pero para todos los demás objetos que se guardan en el caché existe el problema de cuánto tiempo deben quedarse allí. Para determinarlo se asignan diferentes estados a los objetos del caché.

Los servidores web y los cachés proxy controlan el estado de un objeto añadiendo cabeceras como `Last modified` (última modificación) o `Expires` (expira) y la fecha correspondiente. También se utilizan otras cabeceras para especificar los objetos que no deben cachearse.

Normalmente, los objetos desaparecerán antes del caché por la falta de espacio en el disco. Se utiliza algoritmos para sustituir objetos en el caché, como el LRU (Last Recently Used) que consiste en sustituir los objetos menos utilizados por nuevos.

Requerimientos del sistema

Lo más importante es cuantificar la carga que va a tener que soportar nuestro sistema. Para esto es importante fijarse más en los picos de carga del sistema que en la media total, ya que los picos pueden llegar a ser varias veces la media del día. En caso de duda siempre es mucho mejor sobreestimar los requerimientos del sistema, ya que un Squid trabajando al límite de su capacidad puede repercutir negativamente en el funcionamiento de los servicios.

Discos duros

Cuando se trata de cachés, la velocidad es un parámetro importantísimo. En los discos duros este parámetro se mide mediante su "tiempo medio de acceso" (en inglés `random-seek time`) en milisegundos, que debe ser lo más bajo posible.

Otra posibilidad para aumentar la velocidad consiste en el uso paralelo de varios discos duros o de una estructura raid.

Tamaño del caché de disco

Depende de varios factores. En un caché pequeño la probabilidad de un HIT (el objeto ya se encuentre en el caché) será pequeña, ya que el caché se llenará con facilidad y se deberá sustituir los objetos antiguos por nuevos. En cambio, en el caso de disponer de por ejemplo 1 GB de disco para cachear, y de que los usuarios sólo necesiten 10 MB al día para navegar, se tardará al menos 100 días en llenar el caché.

El método más fácil para determinar el tamaño del caché es en función del tráfico máximo que pase por el mismo. Si disponemos de una conexión de 1 Mb/s, como mucho se transferirán 125 KB por segundo. Si todo este tráfico va a parar al caché, en una hora será 450 MB, y suponiendo que este tráfico se genera durante las 8 horas de trabajo, tendremos en total 3.6 GB diarios. Como la línea no suele trabajar al máximo, la cantidad total de datos procesada por el caché es de unos 2 GB. Así pues, para guardar todos los datos navegados por la WWW en un día, necesitamos en este ejemplo 2 GB de espacio en disco para Squid.

Debido a que en la mayoría de los casos Squid lee o escribe pequeños bloques del disco duro, el tiempo de acceso del disco duro es más importante que su capacidad de transferencia de datos. Precisamente en este contexto muestran su valía los discos duros con una alta velocidad de rotación, ya que permiten un posicionamiento más rápido de la cabeza de lectura.

Memoria RAM

La cantidad de memoria requerida por Squid está relacionada directamente con la cantidad de objetos que se encuentran en el caché. Squid también almacena referencias a los objetos en el caché y objetos utilizados frecuentemente en la memoria RAM para optimizar la obtención de los mismos. La memoria RAM es muchísimo más rápida que el disco duro.

Squid también guarda muchos otros datos en la memoria, como por ejemplo una tabla con todas las direcciones IP utilizadas, un caché para los nombres de dominio totalmente cualificados, objetos "calientes" (los que más se solicitan), buffers, listas de control de acceso, etc.

Es muy importante tener memoria más que suficiente para el proceso de Squid, ya que en el caso de tener que pasar el proceso al disco duro, las prestaciones del sistema se reducirán drásticamente. Para facilitar la administración de la memoria utilizada por el caché, podemos utilizar la herramienta `cachemgr.cgi` tal y como veremos en el apartado [cachemgr.cgi](#) en la página 489.

Potencia del procesador

Squid no es un programa que consuma mucho CPU. Solamente al arrancar y comprobar el contenido del caché es cuando se trabaja más intensamente con el procesador. El uso de máquinas con multiprocesador tampoco incrementa el rendimiento del sistema. Para obtener una mayor efectividad, es preferible aumentar la cantidad de memoria RAM o bien utilizar discos más rápidos antes que cambiar el procesador por otro más potente.

Algunos ejemplos de sistemas configurados y que utilizan Squid se encuentran disponibles en <http://wwwcache.ja.net/servers/squids.html>.

Arrancar Squid

Squid ya se encuentra preconfigurado en SuSE Linux así que casi se puede iniciar directamente después de la instalación. Los requisitos en este caso son: tener una red ya configurada, al menos un servidor de nombres, y, por supuesto, acceso a Internet. Pueden aparecer problemas en caso de utilizar una conexión telefónica que utilice configuración dinámica de DNS. En casos como éste, al menos el servidor de nombres debe estar claramente especificado, ya que Squid solamente se iniciará si detecta un servidor DNS en el archivo `/etc/resolv.conf`.

Para iniciar Squid, introduzca desde la línea de comandos como usuario `root`:

```
rcsquid start
```

Durante el primer inicio del programa se define la estructura de directorios en `var/squid/cache`. Esta operación es llevada a cabo automáticamente por el script de inicio `/etc/rc.d/squid` y puede tardar desde pocos segundos a minutos. Cuando aparezca el mensaje `done` en color verde a la derecha de la pantalla, significa que Squid ya ha sido cargado. Se puede comprobar si Squid funciona correctamente en el sistema local dando los valores `localhost` y `port 3128` como proxy en cualquier navegador web. Para permitir a todos los usuarios el acceso a Squid y por tanto a Internet, solamente es necesario cambiar una entrada en el archivo de configuración `/etc/squid/squid.conf` de `http_access deny all` a `http_access allow all`. Sin embargo, haciendo esto Squid se hace accesible para cualquiera. Por tanto, en cualquier caso deberá configurar listas de control de acceso o ACL para controlar el acceso al proxy. Más información sobre este tema en el apartado *Listas de control de acceso o ACLs* en la página 483.

Cada vez que se produce un cambio en el archivo de configuración `/etc/squid/squid.conf`, hay que decirle a Squid que a partir de este momento

debe utilizar el nuevo archivo de configuración. Esto se puede hacer con el siguiente comando:

```
rcsquid reload
```

O bien reiniciar completamente Squid:

```
rcsquid restart
```

Los siguientes comandos son igualmente importantes:

```
rcsquid status
```

El comando superior permite determinar si el proxy se encuentra funcionando y con

```
rcsquid stop
```

se puede parar Squid. Este último comando puede tardar unos momentos ya que Squid espera hasta medio minuto (opción `shutdown_lifetime` en `/etc/squid/squid.conf`) antes de cortar las conexiones con los clientes y entonces todavía tendrá que guardar los datos en el disco.

Aviso

Terminar Squid

En caso que Squid sea terminado con un comando `kill` o bien `killall`, esto puede llevar a la destrucción del caché, que en ese caso tendrá que ser borrado completamente para poder reiniciar Squid

Aviso

Si Squid finaliza de forma inesperada tras un corto periodo de tiempo aunque pareciera que se había iniciado correctamente, puede ser debido a una entrada de DNS incorrecta o bien por no encontrar el archivo `/etc/resolv.conf`. Squid almacena la causa del error en el archivo `/etc/rc.config`.

Si Squid debe cargarse automáticamente cada vez que se inicie el sistema, solamente es necesario activarlo en el "editor de niveles de ejecución" de YaST.

Al desinstalar Squid no se borrará ni el caché ni los archivos de error. Se deberá borrar manualmente el directorio `/var/cache/squid`.

Servidor DNS local

Configurar un servidor DNS localmente como BIND-9 es igualmente importante, incluso aunque el servidor proxy no controle su propio dominio. En ese

caso actuará solamente como “caché-solamente DNS” y de esta manera será capaz de resolver peticiones DNS a través del servidor de nombres principal sin necesidad de realizar ninguna configuración especial. Si introduce en el archivo `/etc/resolv.conf` una entrada con dirección IP `127.0.0.1` para `localhost`, Squid detectará un servidor de nombres válido al iniciarse. La configuración de un servidor DNS ya es un capítulo en si misma y no será descrita con detalle en este capítulo. Será suficiente instalar el paquete e iniciarlo. El servidor de nombres del proveedor deberá especificarse en el archivo de configuración `/etc/named.conf` bajo `forwarders` junto con su dirección IP. En caso de disponer de un cortafuegos activado, incluso aunque se trate del cortafuegos personal, tendrá que asegurarse que deje pasar las peticiones DNS.

El archivo de configuración `/etc/squid/squid.conf`

La configuración de Squid se almacena en este archivo de configuración. Para poder iniciar Squid por primera vez, no es necesario hacer cambios en este archivo, aunque los clientes externos tendrán inicialmente el acceso denegado. El proxy necesita ejecutarse en `localhost` y normalmente utilizará el puerto 3128. Las opciones son muy extensas y están documentadas con muchos ejemplos en el archivo `/etc/squid/squid.conf` preinstalado. Casi todas las líneas comienzan por el símbolo `#` (significa que la línea está comentada y su contenido no se evaluará); las opciones relevantes se encuentran al final de la línea. Los valores por defecto corresponden casi siempre a los valores que necesitaremos, así que para muchas opciones sólo será necesario quitar el símbolo de comentario al principio de la líneas. De cualquier modo, es mejor dejar el ejemplo comentado y reescribir la línea con los nuevos parámetros una línea más abajo. De esta manera se puede ver fácilmente cuales son los valores por defecto y cuales son los cambios introducidos.

Atención

Actualización de la versión 2.4 a la versión 2.5

Después de actualizar Squid de la versión 2.4 a la versión 2.5 es necesario borrar el caché de Squid, ya que el esquema de la estructura de directorios ha cambiado.

Atención

Si está actualizando desde una versión anterior de Squid, se recomienda editar el nuevo `/etc/squid/squid.conf` y añadirle la configuración del archivo anterior. Si trata de implementar directamente el antiguo archivo de configuración `/etc/squid.conf`, es posible que no funcione correctamente debido a modificaciones en algunas opciones o a los nuevos cambios en la nueva versión.

Opciones generales de configuración (selección)

http_port 3128 Este es el puerto en el que Squid escuchará las peticiones de los clientes. El puerto por defecto es 3128, aunque 8080 se usa también comúnmente. Es posible especificar varios puertos separándolos por espacios en blanco.

cache_peer <hostname> <tipo> <puerto-proxy> <puerto-icp> En esta opción podemos especificar otro servidor proxy como "padre" (ingl. parent) si lo desea o si prefiere usar el de su proveedor o ISP. En la opción <hostname>, se especifica el nombre y la dirección IP del proxy al que nos vayamos a conectar, en la opción <tipo>, especificamos parent. Para <puerto-proxy>, se debe escribir el número de puerto, el que también se especifica para los navegadores, normalmente se utiliza el 8080. Se puede fijar el <puerto-icp> a 7 o bien 0 si no se conoce el puerto ICP del proxy padre y su uso carece de interés para el proveedor. Además de esto, default y no-query se deben especificar después de los números de puerto para no permitir el uso del protocolo ICP. Squid se comportará en ese caso como un navegador normal en lo que respecta al proxy del proveedor.

cache_mem 8 MB Esta entrada define la cantidad máxima de memoria RAM que utilizará Squid para los cachés. El valor por defecto es 8 MB.

cache_dir ufs /var/cache/squid 100 16 256 La entrada correspondiente a cache_dir fija el directorio donde se almacenarán los datos. Los números al final indican el tamaño máximo en MB que se va a utilizar, seguido del número de directorios de primer y segundo nivel. El parámetro ufs debe dejarse tal y como está. El valor por defecto es 100 MB de espacio en disco ocupado en el directorio /var/cache/squid, para luego crear 16 subdirectorios más, y en cada uno de ellos se crearán 256 directorios más. Al especificar el espacio de disco a utilizar, siempre se debe dejar espacio suficiente de reserva. Se recomienda manejar valores de tamaño para el caché entre el 50 a un 80 por ciento del espacio total disponible. Los últimos dos números sólo deben ser incrementados con precaución ya que demasiados directorios pueden provocar problemas de funcionamiento. En caso de disponer de más discos para repartir entre ellos el caché, se pueden especificar varias líneas de cache_dir.

cache_access_log /var/log/squid/access.log ruta para archivos log.

cache_log /var/log/squid/cache.log ruta para archivos log.

cache_store_log /var/log/squid/store.log ruta para archivos log.

Estas tres entradas especifican la ruta donde Squid guardará sus archivos de registro. Normalmente no hace falta cambiar nada. Si Squid soporta una carga relativamente elevada, puede ser necesario distribuir el caché y estos archivos de registro en discos diferentes.

emulate_httpd_log off Si la entrada está configurada a **on**, se puede obtener archivos de log en formato legible. Sin embargo, algunos programas de evaluación no pueden interpretarlos.

client_netmask 255.255.255.255 Con esta entrada, es posible enmascarar las direcciones IP en los archivos de control para ocultar la identidad de los clientes. Especificando en esta opción el valor **255 . 255 . 255 . 0**, el último dígito de la dirección IP se interpretará como cero.

ftp_user Squid@ Con esta opción se puede fijar la contraseña que Squid utilizará para realizar el registro (ingl. login) para FTP anónimo. Es importante especificar una dirección de correo electrónico válida, ya que algunos servidores FTP pueden comprobar si es válida o no.

cache_mgr webmaster Dirección de correo electrónico a la que el Squid enviará un mensaje en caso que termine inesperadamente. Por defecto se enviarán al webmaster.

logfile_rotate 0 Squid puede rotar archivos de registro al ejecutar la orden **squid -k rotate**. Los archivos serán enumerados en este proceso y después de alcanzar el valor especificado, el archivo más antiguo será sobrescrito. El valor que se utiliza normalmente es **0** ya que para archivar y borrar archivos de registro en SuSE Linux se utiliza un cronjob que se puede encontrar en el archivo de configuración **/etc/logrotate/syslog**.

append_domain <dominio> Con la opción **append_domain**, se puede especificar qué dominio se añadirá automáticamente en caso de que no se facilite ninguno. Normalmente se especifica el propio dominio, de forma que basta con introducir **www** en el navegador para acceder al servidor web propio.

forwarded_for on Al apagar esta opción y ponerla a **off**, Squid eliminará las direcciones IP y el nombre de la máquina de los clientes en las peticiones HTTP.

negative_ttl 5 minutes; negative_dns_ttl 5 minutes Normalmente no es necesario cambiar estos valores. En caso de disponer de una conexión telefónica puede ser que a veces no se pueda acceder a Internet. Squid tomará nota de las peticiones fallidas y se negará a realizarlas otra vez, incluso

aunque la conexión ya se haya restablecido. En ese caso puede cambiar el valor `minutes` a `seconds`. Después de esto, al pulsar en el botón de **Recargar** en el navegador la conexión se reiniciará al cabo de unos segundos.

never_direct allow <acl_name> Si desea impedir que Squid conteste a peticiones que vengan directamente de Internet, puede utilizar el siguiente comando para forzar la conexión a otro proxy. Éste debe estar ya introducido en la opción `cache_peer`. Si se especifica como `<acl_name>` el valor `all`, todas las peticiones serán redirigidas al caché padre. Esto puede ser necesario, por ejemplo, en caso de disponer de un proveedor que estipule estrictamente el uso de sus proxys o que no permita acceso directo a Internet a través de su cortafuegos.

Listas de control de acceso o ACLs

Squid implementa un inteligente sistema para controlar el acceso al proxy que puede configurarse fácil y detalladamente mediante las ACLs. Se trata de normas procesadas secuencialmente. Las ACLs deben ser definidas antes de poderse utilizar. Algunas ACLs como `all` y `localhost` ya están definidas.

La mera definición de una ACL no tiene ningún efecto. Es necesario que se ponga en funcionamiento p. ej. con `http_access` para que puedan procesarse las reglas definidas anteriormente.

acl <acl_nombre> <tipo> <datos> Una ACL necesita por lo menos tres especificaciones para definirla. El nombre `<acl_nombre>` se puede elegir arbitrariamente. Para el `<tipo>` se puede elegir de entre diferentes opciones disponibles en la sección **ACCESS CONTROLS** del archivo `/etc/squid/squid.conf`. La parte de datos depende del tipo de ACL y también puede ser leída desde un archivo, p. ej. que contenga nombres de máquinas, direcciones IP o bien URLs. A continuación unos ejemplos:

```
acl usuarios srcdomain .mi-dominio.com
acl profesores src 192.168.1.0/255.255.0.0
acl alumnos src 192.168.7.0-192.168.9.0/255.255.0.0
acl mediodía time MTWHF 12:00-15:00
```

http_access allow <acl_nombre> `http_access` define a quién le está permitido usar el proxy y quién puede acceder a Internet. Para todo esto se deberán definir primero las ACL correspondientes. `localhost` y `all` ya han sido definidas con anterioridad. En general se puede permitir el acceso mediante `allow` o bien negarlo con `deny`. Se puede crear una lista

completa de entradas `http_access` que será procesada de arriba hacia abajo y dependiendo de cómo estén configuradas las reglas se podrá acceder o no a Internet para cada URL. Por eso la última entrada de todas debe ser `http_access deny all`. En el ejemplo siguiente `localhost` dispone de acceso libre mientras que todos los otros hosts tienen el acceso denegado.

```
http_access allow localhost
http_access deny all
```

Otro ejemplo donde se utilizan las reglas definidas anteriormente: el grupo `profesores` siempre tendrá acceso a Internet, mientras que el grupo `alumnos` solamente tiene acceso de lunes a viernes durante el mediodía.

```
http_access deny localhost
http_access allow profesores
http_access allow alumnos mediodía time
http_access deny all
```

Esta lista con las entradas para `http_access` deberá colocarse en la parte del archivo `/etc/squid/squid.conf` a partir de la entrada

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
# CLIENTS
```

y finalizar en

```
http_access deny all
```

redirect_program /usr/bin/squidGuard Con esta opción se puede especificar un programa de redirección como `squidGuard` capaz de bloquear el acceso a URL no deseadas. El acceso a Internet puede ser controlado individualmente para varios grupos de usuarios con la ayuda de autenticación por proxy y listas de control de acceso apropiadas. `squidGuard` es un paquete independiente que se debe instalar y configurar separadamente.

authenticate_program /usr/sbin/pam_auth Si los usuarios deben ser autenticados en el proxy, se puede especificar un programa que realice esta función como `pam_auth`. Cuando se accede a `pam_auth` por primera vez, el usuario verá una pantalla de login donde se deberá introducir el nombre de usuario y la contraseña. Además será necesario especificar una ACL correspondiente para que sólo los usuarios registrados puedan acceder a Internet:


```
acl password proxy_auth REQUIRED
```

```
http_access allow password  
http_access deny all
```

El texto **REQUIRED** después de **proxy_auth** debe ser sustituido por una lista de usuarios permitidos o por la ruta a una lista.

ident_lookup_access allow <acl_nombre> Con esta opción se consigue que para todos los clientes que pertenezcan a la ACL especificada se ejecute un programa que determine la identidad del cliente. Al especificar el valor **all** como **<acl_nombre>**, esto será válido para todos los clientes. Para esto deberá ejecutar un daemon denominado **ident** en todos los clientes. En Linux, se puede utilizar para este propósito el paquete **pidentd**; para Windows, hay software libre disponible que se puede descargar de Internet. Para asegurar que sólo se permite acceso a clientes correctamente identificados, se deberá igualmente especificar otra ACL tal y como se define a continuación:

```
acl idenhosts ident REQUIRED
```

```
http_access allow idenhosts  
http_access deny all
```

Aquí también se puede cambiar el valor **REQUIRED** por una lista de usuarios autorizados. El uso de **ident** puede reducir la velocidad del sistema debido a que el proceso de autenticación se repite para cada petición.

Configuración de un proxy transparente

Normalmente la forma en la que se trabaja con servidores proxy es la siguiente: el navegador web envía peticiones a un puerto determinado del servidor proxy, y éste se encarga de servirle las páginas, se encuentren o no en su caché. A la hora de trabajar con una red real se pueden dar los siguientes casos:

- Por motivos de seguridad, es más seguro que todos los usuarios utilicen un proxy para navegar por Internet.
- Se requiere que todos los usuarios utilicen un proxy, sean los usuarios conscientes de ello o no.
- Si el proxy de una red cambia de ubicación, los clientes existentes mantienen su antigua configuración.

En cualquiera de estos casos se puede utilizar un proxy transparente. El principio es muy sencillo: el proxy intercepta y responde a las peticiones del navegador web, así que el navegador recibirá las páginas solicitadas sin saber exactamente de dónde provienen. El proceso completo se realiza de forma transparente, de ahí el nombre que este procedimiento recibe.

Configuración del kernel

Primero hay que comprobar que el kernel del servidor proxy dispone de soporte para proxy transparente. En caso contrario habrá que añadir estas opciones al kernel y compilarlo de nuevo. Más detalles sobre este proceso en el capítulo [El kernel de Linux](#) en la página 255.

Los módulos del kernel cambian en cada versión. Compruebe el estado del actual en `/usr/share/doc/howto/en/html/mini/TransparentProxy-3.html` o en Internet: <http://www.tldp.org/HOWTO/mini/TransparentProxy-3.html>. Ahora debe grabar la nueva configuración, compilar el nuevo kernel, instalarlo y configurar nuevamente LILO si hace falta. Finalmente, se deberá reiniciar el sistema.

Opciones de configuración en `/etc/squid/squid.conf`

Ahora vamos a ocuparnos de las opciones que hay que activar en el archivo `/etc/squid/squid.conf` para activar el proxy transparente.

Las opciones son:

- `httpd_accel_host virtual`
- `httpd_accel_port 80` # número de puerto del servidor HTTP
- `httpd_accel_with_proxy on`
- `httpd_accel_uses_host_header on`

Configuración del cortafuegos con SuSEfirewall2

Ahora sólo falta redirigir las peticiones de los clientes por el cortafuegos hacia el puerto en el que está Squid.

Para la configuración utilizaremos la herramienta proporcionada por SuSE SuSEfirewall2. El archivo de configuración correspondiente se encuentra en `/etc/sysconfig/scripts/SuSEfirewall2-custom`. Este archivo está formado por diferentes entradas muy bien documentadas. Tendremos que configurar algunas opciones más. En nuestro ejemplo:

- Dispositivo apuntando a Internet: FW_DEV_EXT="eth1"
- Dispositivo apuntando a la red: FW_DEV_INT="eth0"

Se accederá a los puertos y servicios (ver /etc/exports) del cortafuegos desde redes no seguras como Internet. En este ejemplo sólo se especifican servicios web hacia el exterior:

```
FW_SERVICES_EXT_TCP="www"
```

Se accederá a los puertos y servicios (ver /etc/exports) del cortafuegos desde la red segura. Tanto TCP como UDP:

```
FW_SERVICES_INT_TCP="domain www 3128"
```

```
FW_SERVICES_INT_UDP="domain"
```

Accedemos a servicios web y al programa Squid (cuyo puerto por defecto es 3128). El servicio "domain" especificado anteriormente se trata del DNS o Domain Name Server. Lo más normal es utilizar este servicio, pero en caso contrario, se elimina de las entradas superiores y se configura la opción siguiente a no:

```
FW_SERVICE_DNS="yes"
```

La opción más importante es la número 15:

```
#
# 15.)
# Which accesses to services should be redirected to a localport
# on the firewall machine?
#
# This can be used to force all internal users to surf via your
# squid proxy, or transparently redirect incoming webtraffic to
# a secure webserver.
#
# Choice: leave empty or use the following explained syntax of
# redirecting rules, separated by a space.
# 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"
#
```

Fichero 49: Opción 15 de la configuración del cortafuegos

Los comentarios indican la sintaxis que hay que seguir. En primer lugar, se escribe la dirección IP y la máscara de las "redes internas" de donde vienen nuestros datos. En segundo lugar, la dirección IP y la máscara de red a donde se "dirigen" las peticiones. En el caso de navegadores web, especificaremos la dirección de red 0/0, un comodín que quiere decir "a cualquier dirección". A continuación, el número de puerto "original" al que se dirigen las peticiones, y finalmente, el puerto a donde "redirigimos" las peticiones.

Como Squid tiene soporte para más protocolos además de http; existe la posibilidad de desviar las peticiones dirigidas a otros puertos al proxy, como por ejemplo FTP (puerto 21), HTTPS o SSL (Puerto 443).

En el ejemplo dado, los servicios web (puerto 80) se desvían al puerto del proxy (aquí 3128). En el caso de disponer de más redes para añadir, sólo hace falta separar las diferentes entradas con un espacio en blanco en la línea correspondiente.

```
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 que el cortafuegos se inicie y con él la nueva configuración, se debe editar una entrada en el archivo `/etc/sysconfig/SuSEfirewall2` y asignar el valor "yes" a la entrada `FW_START`:

Inicie Squid tal como se mostró en el apartado [Arrancar Squid](#) en la página 478. Para comprobar que todo funciona correctamente, compruebe los archivos de registro de Squid en `/var/log/squid/access.log`

Para verificar que todos los puertos están correctamente configurados, se puede realizar un escaneo de puertos en la máquina desde un ordenador que se encuentre fuera de la red local. Sólo deberá estar abierto el puerto de servicios web (80). Para llevar a cabo el portscan se puede utilizar `nmap` con la siguiente sintaxis:

```
nmap -0 direccion_IP
```

Squid y otros programas

En esta sección veremos cómo otros programas interactúan con Squid. `cachemgr.cgi` permite al administrador del sistema comprobar la cantidad de memoria necesaria para cachear los objetos, `squidGuard` filtra páginas web, y `calamaris` es un generador de informes para Squid.

cachemgr.cgi

El administrador de caché (cachemgr.cgi) es una utilidad CGI para mostrar estadísticas sobre el consumo de memoria del proceso Squid. Este método representa una forma más sencilla de controlar el uso del caché y ver estadísticas sin necesidad de registrarse en el servidor.

Configuración

En primer lugar, se necesita tener un servidor web ejecutándose en el sistema. Para comprobar si Apache está funcionando, escriba como usuario `root`:

```
rcapache status.
```

Si aparece un mensaje como el siguiente:

```
Checking for service httpd: OK
Server uptime: 1 day 18 hours 29 minutes 39 seconds
```

Es porque Apache ya se está ejecutando en su máquina. Si no es así, escriba:

```
rcapache start
```

para iniciar Apache con la configuración por defecto de SuSE Linux.

El último paso es copiar el archivo `cachemgr.cgi` al directorio de Apache para las `cgi-bin`:

```
cp /usr/share/doc/packages/squid/scripts/cachemgr.cgi
/srv/www/cgi-bin/
```

Opciones en `/etc/squid/squid.conf`

Hay algunas opciones configuradas ya por defecto en el archivo de configuración para el administrador de caché:

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
```

Con las siguientes normas de acceso:

```
http_access allow manager localhost
http_access deny manager
```

La primera ACL es la más importante, ya que el administrador de caché tratará de comunicarse con Squid mediante el protocolo `cache_object`.

Las reglas siguientes asumen que el servidor web y Squid se encuentran en la misma máquina. Si la comunicación entre el administrador de caché y Squid se origina en el servidor de web en otro ordenador, tendremos que incluir una ACL adicional como en la figura 50.

```
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 # IP del servidor web
```

Fichero 50: Añadiendo una ACL adicional

Entonces hay que añadir las reglas siguientes como en la figura 51.

```
http_access allow manager localhost
http_access allow manager webserver
http_access deny manager
```

Fichero 51: Reglas de acceso

Igualmente también se puede configurar una contraseña para el administrador si deseamos tener acceso a más opciones, como por ejemplo poder cerrar el caché de forma remota o ver más información sobre el mismo. En ese caso sólo hay que configurar la entrada `cachemgr_passwd` con una contraseña para el administrador y la lista de opciones que deseamos ver. Esta lista aparece como una parte de los comentarios a la entrada en `/etc/squid/squid.conf`.

Cada vez que se modifique el archivo de configuración es necesario reiniciar Squid. Utilice para ello el comando

```
rcsquid reload
```

Leer las estadísticas

En primer lugar, diríjase a la página web correspondiente:

<http://miservidor.ejemplo.org/cgi-bin/cachemgr.cgi>

Pulse en 'continue' y navegue a través de las diferentes estadísticas. Hay más detalles para cada entrada mostrada por el administrador de cachés en la FAQ de Squid en la <http://www.squid-cache.org/Doc/FAQ/FAQ-9.html>

squidGuard

Este capítulo no pretende mostrar una configuración completa de squidGuard, sino más bien presentarlo y comentar su utilización. Para ver las opciones de configuración con más detalle, visite la web de squidGuard en <http://www.squidguard.org>.

squidGuard es un programa gratuito, bajo licencia GPL, que funciona como un filtro flexible ultra rápido capaz de redireccionar páginas web y que funciona como "plugin de control de acceso" para Squid. Permite definir diversas reglas de acceso con diferentes restricciones para distintos grupos de usuarios que trabajen sobre un caché de Squid. squidGuard utiliza la interfaz estándar de redirección de Squid.

Algunos ejemplos de utilización de squidGuard:

- Limitar el acceso por web para una serie de usuarios a una lista de servidores web o URL conocidas y aceptadas.
- Bloquear el acceso para algunos usuarios a servidores web o URLs que estén en alguna lista negra.
- Bloquear para algunos usuarios el acceso a URLs que coincidan con una determinada lista de expresiones o palabras.
- Redireccionar URLs bloqueadas a una página de información "inteligente" basada en CGI.
- Redireccionar usuarios no registrados a una página de registro.
- Redireccionar banners a un GIF vacío.
- Tener diferentes normas de acceso basadas en la hora del día, día de la semana, etc.
- Tener diferentes normas para diferentes grupos de usuarios.
- Y muchas más..

Ni squidGuard ni Squid se pueden usar para:

- Editar, filtrar o censurar texto dentro de documentos.
- Editar, filtrar o censurar lenguajes de script con HTML embebido como JavaScript o VBscript.

Utilizar squidGuard

Instale el paquete `squidgrd`. Edite un archivo mínimo de configuración `/etc/squidguard.conf`. Hay muchos ejemplos diferentes de configuración en <http://www.squidguard.org/config/>. Siempre se puede experimentar más tarde con configuraciones más complicadas.

El paso siguiente es crear una página web que será la página que mostrará el mensaje de "acceso denegado" o una página CGI más o menos inteligente a la cual redirigir Squid en caso que algún cliente pida algún sitio web que esté en la lista negra. Una vez más, el uso de Apache es altamente recomendable.

Ahora debemos decirle a Squid que utilice squidGuard. Lo haremos mediante las siguientes entradas en el archivo `/etc/squid/squid.conf`:

```
redirect_program /usr/bin/squidGuard
```

Existe todavía otra opción llamada `redirect_children` que configura el número de procesos diferentes para "redirigir" (en este caso procesos de squidGuard). squidGuard es suficientemente rápido para procesar grandes cantidades de solicitudes (squidGuard es realmente rápido: 100.000 consultas en 10 segundos en un Pentium 500MHz con 5.900 dominios, 7.880 URLs, en total 13.780). Por eso no se recomienda configurar más de cuatro procesos a la vez para no gastar memoria innecesariamente en la asignación de los procesos.

```
redirect_children 4
```

Por último vuelva a cargar la configuración de Squid:

```
rcsquid reload
```

A continuación ya se puede comprobar la configuración con cualquier navegador.

Generación de informes con Calamaris

Calamaris es un script en Perl utilizado para generar informes de la actividad del caché en formatos ASCII o HTML. Funciona directamente con los archivos de registro de acceso de Squid. La página web de Calamaris está en <http://Calamaris.Cord.de/>

La utilización del programa es bastante fácil. Entre al sistema como `root` y ejecute:

```
cat access.log.files | calamaris [options] > reportfile
```

Al enviar más de un archivo de registro es importante que éstos estén cronológicamente ordenados, es decir, primero los archivos más antiguos.

Las diferentes opciones:

- a utiliza todos los informes disponibles
- w muestra los resultados en formato HTML
- l muestra un mensaje o un logotipo en la cabecera del informe

Puede obtener más información sobre las diferentes opciones del programa en la página de manual de calamaris: `man calamaris`

Un ejemplo típico:

```
cat access.log.2 access.log.1 access.log | calamaris -a -w \  
>/usr/local/httpd/htdocs/Squid/squidreport.html
```

Colocamos el informe en el directorio del servidor web. Otra vez es necesario el programa Apache para ver los informes.

Otro completo generador de informes es SARG (Squid Analysis Report Generator). Más información sobre SARG se puede encontrar en las páginas web correspondientes en: <http://web.onda.com.br/orso/>

Información adicional sobre Squid

Visite la página web de Squid: <http://www.squid-cache.org/>. Aquí encontrará la Guía de Usuario de Squid y una extensa colección de FAQ sobre Squid.

El Mini-Howto sobre proxys transparentes se encuentra en el paquete `howtoen`, bajo `/usr/share/doc/howto/en/mini/TransparentProxy.gz`

También existen listas de correo para Squid en: squid-users@squid-cache.org.

El archivo para estas listas se encuentra en: <http://www.squid-cache.org/mail-archive/squid-users/>

Seguridad en la red

Enmascarar (ingl. *masquerading*), cortafuegos (ingl. *firewall*) y "Kerberos" constituyen los fundamentos de una red segura en la que el tráfico de datos se encuentra bajo control. La SSH, (ingl. *Secure Shell*), ofrece al usuario la oportunidad de realizar una conexión codificada con un ordenador remoto. En el apartado que viene a continuación, le explicamos cómo puede utilizar este gran abanico de posibilidades.

Cortafuegos y masquerading	496
SSH – secure shell, la alternativa segura	502
Autenticación en la red — Kerberos	508
Instalación y administración de Kerberos	515
La seguridad, una cuestión de confianza	532

Cortafuegos y masquerading

Debido a las extraordinarias características de Linux en lo que se refiere a redes, este sistema se utiliza cada vez más como enrutador (ingl. *router*) en conexiones tanto adicionales como estándar. Con el concepto de "enrutador" nos referimos aquí a un ordenador que tiene más de una interfaz de red y que reenvía paquetes que no son para una de sus propias interfaces de red a sus equivalentes en otras redes. A menudo a un enrutador se le denomina "pasarela" (ingl. *gateway*). Los filtros de paquetes disponibles en el kernel de Linux posibilitan un control adecuado sobre los paquetes del tráfico de datos en la red a los que se permite pasar y a los que no.

La configuración de las normas adecuadas para este filtrado de datos requiere algo de experiencia por parte del administrador. SuSE Linux incluye, para los usuarios con menos experiencia un paquete independiente que facilitan la configuración de estas normas: paquete `SuSEfirewall2`.

`SuSEfirewall2` puede configurarse con gran flexibilidad, lo que le hace muy apropiado para la construcción de complejos filtros.

Mediante esta solución de filtro de paquetes y por medio de masquerading, un ordenador Linux puede actuar como enrutador para unir una red interna a una única dirección IP visible desde el exterior a través de una línea telefónica o dedicada. El masquerading se lleva a cabo con ayuda de las normas del filtrado de paquetes.

Aviso

Este capítulo describe un procedimiento estándar que debería funcionar correctamente en la mayoría de los casos. Sin embargo, aunque la información es lo más exacta y completa posible, no se ofrece ninguna garantía. SuSE no asume ninguna responsabilidad sobre el éxito o fracaso de sus medidas de seguridad. Le agradecemos de antemano sus críticas y sugerencias. Aún cuando no reciba una respuesta directa de nuestra parte, puede estar seguro de que agradecemos la crítica y las sugerencias y de que intentaremos incorporar las mejoras.

Aviso

Fundamentos del masquerading

Masquerading es la adaptación a Linux de NAT (Network Address Translation), la traducción de direcciones de red. El principio en el que se sustenta no es muy complicado: Su enrutador tiene más de una interfaz de red, que por

regla general suelen ser una tarjeta de red y un módem (o una interfaz RDSI). Vd. se conecta con el exterior por medio de una de estas interfaces; otra u otras conectan su ordenador con otros ordenadores en su misma red. Por ejemplo, se debe conectar al exterior vía RDSI y la interfaz de red exterior es `ipp0`. Vd. tiene más de un ordenador en la red local conectados con la tarjeta de red de su enrutador Linux, que en este ejemplo es `eth0`. Los ordenadores de la red reenvían todos los paquetes que no son para la propia red al enrutador o pasarela (ingl. *gateway*) por defecto.

Atención

¡Al configurar su red, tenga cuidado siempre con direcciones de retransmisión (ingl. *broadcast*) y máscaras de red coincidentes!

Atención

Si uno de los ordenadores de su red envía un paquete a Internet, éste aterrizará en el enrutador por defecto. Éste debe estar configurado de tal manera que reenvía dichos paquetes. ¡Por razones de seguridad, una instalación de SuSE-Linux no lo hará! Modifique la variable `IP_FORWARD` en el fichero `/etc/sysconfig/sysctl` y asígnele el valor `IP_FORWARD=yes`. Para que el reenvío se active, debe reiniciar o escribir el siguiente comando:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

La máquina destino sólo conoce el enrutador, y no el ordenador en sí de su red interna desde la que se envió el paquete, puesto que esta queda escondida detrás del enrutador. De ahí viene el concepto "enmascarar" (ingl. *masquerading*). Debido a la traducción de direcciones, la dirección de destino del paquete de respuesta es de nuevo el enrutador. Este debe reconocer el paquete y modificar la dirección de destino para que aterrice en el ordenador correcto de la red local.

Este reconocimiento de paquetes, de conexiones originadas por el masquerading del enrutador, ocurre con ayuda de una tabla que se mantiene directamente en el kernel del enrutador, mientras las conexiones correspondientes estén activas. El superusuario (`root`) puede ver estas tablas con los comandos `ipchains` o `iptables`. Consulte estos comandos en las páginas man para encontrar indicaciones más precisas. A la hora de identificar una determinada conexión "enmascarada", también son importantes las direcciones del remitente y de destino, así como el número de protocolo y los protocolos que participan. Con todo esto es posible que su enrutador pueda "esconder" simultáneamente varios miles de conexiones para cada uno de los ordenadores locales.

Puesto que el camino que realizan los paquetes de fuera adentro depende de las tablas del masquerading, no hay ninguna posibilidad de abrir una conexión desde fuera hacia adentro. No habría ninguna entrada para esta conexión es las

tablas. Una conexión ya establecida tiene un estado asignado en las tablas, de tal forma que esta entrada no pueda ser utilizada por una segunda conexión.

En lo sucesivo esto da lugar a problemas con algunas aplicaciones, como por ejemplo, con ICQ, cucme, IRC (DCC, CTCP), Quake y FTP (en modo PORT). Netscape, el programa estándar de FTP y muchas otras utilizan el modo PASV, que causa pocos problemas con el filtrado de paquetes y el masquerading.

Fundamentos del cortafuegos

El "cortafuegos" (ingl. *firewall*) es de hecho el concepto más extendido para un mecanismo que conecta dos redes y que pretende controlar el tráfico de datos en la medida de lo posible. Existen distintos tipos de cortafuegos que de hecho se diferencian en el nivel lógico y abstracto en el que se examina y controla el tráfico de datos. En realidad, los métodos que presentamos aquí se deberían llamar con más precisión "filtro de paquetes". Un filtro de paquetes regula el pasaje siguiendo criterios como el protocolo, el puerto y la dirección IP. De esta forma, también pueden interceptar paquetes que, debido a las señas que incluyen, no deberían entrar en su red. Por ejemplo, deben interceptar paquetes que tengan como destino el puerto 23 del servicio de telnet de su ordenador. Si quiere, por ejemplo, permitir el acceso a su servidor de web, entonces debe dejar libre el puerto correspondiente. No se examinará el contenido de estos paquetes, si la dirección es la correcta (por ejemplo, que el destino sea su servidor web). El paquete podría contener un ataque a un programa CGI de su servidor web y el filtro de paquetes lo dejaría pasar.

Una construcción eficaz, aunque compleja, es la combinación de distintos tipos de elaboración, por ejemplo, un filtro de paquetes al que se le añaden otras aplicaciones gateway/proxy. El filtro rechazaría paquetes que, por ejemplo, se dirigen a puertos que no están liberados. Sólo dejarían pasar a paquetes para una aplicación gateway. Este proxy actuaría como si fuera el equivalente comunicativo real del servidor que establece una conexión con otros. En este sentido, se puede considerar a un proxy de este tipo como una máquina masquerading en el nivel del protocolo de la aplicación correspondiente. Un ejemplo de este tipo de proxies es Squid, un servidor proxy HTTP, para el que debe configurar su servidor de tal manera que las solicitudes de páginas html pasen primero por la memoria del proxy y, sólo en caso de no encontrar allí la página, se envíen a Internet.

El paquete proxy de SuSE (el paquete proxy-suite de la serie sec) contiene a propósito un servidor proxy para el protocolo FTP.

A continuación nos concentraremos en dos paquetes de filtros de SuSE-Linux. Para más información y enlaces sobre cortafuegos, lea

el Firewall HOWTO, que se incluye en paquete `howtoes`. Si paquete `howtoes` está instalado, también lo puede leer con el comando `less /usr/share/doc/howto/es/Cortafuegos-Como.gz`.

SuSEfirewall2

La configuración de SuSEfirewall2 requiere un cierto grado de experiencia y conocimientos. En `/usr/share/doc/packages/SuSEfirewall2` se encuentra la documentación de SuSEfirewall2.

La configuración se puede realizar con YaST (véase la sección [Configuración con YaST](#) en la página 501) o directamente en el fichero `/etc/sysconfig/SuSEfirewall2`.

Configuración manual

Le guiaremos paso a paso para que pueda realizar una configuración adecuada. En cada punto se indica si es válido para masquerading o para cortafuegos. En los ficheros de configuración también se habla de una DMZ ("zona desmilitarizada"), que no se tratará con más detalle.

En caso de que sólo necesite masquerading, rellene sólo las líneas en las que se indica *Masquerading*.

- Active SuSEfirewall2 con el editor de niveles de ejecución de YaST para su nivel de ejecución (probablemente 3 o 5). De este modo, se introducirán enlaces simbólicos para los scripts `SuSEfirewall2_*` en los directorios `/etc/init.d/rc?.d/`.
- `FW_DEV_WORLD` (firewall, masquerading): Por ejemplo `eth0`, como dispositivo que conduce a Internet. Con RDSI es p.ej. `ipp0`.
- `FW_DEV_INT` (firewall, masquerading): Introduzca aquí el dispositivo que le indica la red interna, "privada". Si no hay ninguna disponibles, déjelo vacío.
- `FW_ROUTE` (firewall, masquerading): Si necesita masquerading, debe introducir `yes` en este punto. Las máquinas internas no serán visibles desde afuera, ya que tienen direcciones de red privadas (p.ej. `192.168.x.x`), que no se muestran en Internet.

Con un cortafuegos sin masquerading, escoja aquí `yes`, si quiere permitir el acceso a la red interna. Para ello, las máquinas internas deben tener direcciones IP asignadas oficialmente. ¡En casos normales, *no* debería permitir el acceso desde fuera a las máquinas internas!

- **FW_MASQUERADE** (masquerading): Si necesita masquerading, introduzca **yes**. Tenga en cuenta que es más seguro es que la red interna acceda a Internet a través de un servidor proxy.
- **FW_MASQ_NETS** (masquerading): Indique aquí el ordenador o red para la que se realizará masquerading. Separe las entradas con un espacio en blanco. Por ejemplo: **FW_MASQ_NETS="192.168.0.0/24 192.168.10.1"**
- **FW_PROTECT_FROM_INTERNAL** (firewall): Introduzca **yes**, si también quiere proteger el ordenador que hace de cortafuegos. Para ello debe dejar libres explícitamente los servicios disponibles para la red interna. Ver también **FW_SERVICES_INTERNAL_TCP** y **FW_SERVICES_INTERNAL_UDP**.
- **FW_AUTOPROTECT_GLOBAL_SERVICES** (firewall): En casos normales déjelo en **yes**.
- **FW_SERVICES_EXTERNAL_TCP** (firewall): Introduzca aquí los servicios a los que se debe tener acceso; p. ej. **"www smtp ftp domain 443"** – para el ordenador en casa que no ofrece ningún servicio no escriba nada.
- **FW_SERVICES_EXTERNAL_UDP** (firewall): Si no utiliza aún un servidor de nombres al que se debe acceder desde fuera, déjelo vacío. En caso contrario, indique aquí los puertos adecuados.
- **FW_SERVICES_INTERNAL_TCP** (firewall): Aquí se definen los servicios a disposición de la red interna. Las entradas son similares a las de **FW_SERVICES_EXTERNAL_TCP**, pero aquí se refieren a la red *interna*.
- **FW_SERVICES_INTERNAL_UDP** (firewall): Ver arriba.
- **FW_TRUSTED_NETS** (firewall): Indique aquí los ordenadores "de confianza" (ingl. *trusted hosts*). Tenga en cuenta que éstos también deben estar protegidos de posibles invasiones. **"172.20.0.0/16 172.30.4.2"** significa que todos los ordenadores cuya dirección IP empieza con **172.20.x.x**, así como el ordenador con la dirección IP **172.30.4.2**, pueden atravesar el cortafuegos.
- **FW_SERVICES_TRUSTED_TCP** (firewall): Indique dirección del puerto TCP que utilizarán los ordenadores de confianza. Escriba p. ej. **1:65535**, si todos los ordenadores de confianza pueden acceder a todos los servicios. Normalmente basta con indicar **SSH** como servicio.
- **FW_SERVICES_TRUSTED_UDP** (firewall): Como arriba, pero en relación a UDP.

- **FW_ALLOW_INCOMING_HIGHPORTS_TCP** (firewall): Si trabaja con un FTP normal (activo), introduzca `ftp-data`.
- **FW_ALLOW_INCOMING_HIGHPORTS_UDP** (firewall): Escriba `dns`, para poder utilizar los servidores de nombres introducidos en `/etc/resolv.conf`. Con `yes` deja libres todos los números altos de puertos.
- **FW_SERVICE_DNS** (firewall): Si dispone de un servidor de nombres, al que debe poder accederse desde fuera, introduzca `yes`; en `FW_TCP_SERVICES_*` se debe liberar el puerto 53.
- **FW_SERVICE_DHCLIENT** (firewall): Si utiliza `dhclient`, para recibir una dirección IP, introduzca `yes`.
- **FW_LOG_***: Aquí puede configurar con lo que quiere hacer el login. Para el sistema en funcionamiento, basta con `yes` en `FW_LOG_DENY_CRIT`.
- **FW_STOP_KEEP_ROUTING_STATE** (firewall): Si accede a Internet automáticamente con `diacd` o vía RDSI (dial on demand), introduzca `yes`.

La configuración ha finalizado. No olvide probar el cortafuegos (p.ej. `telnet` desde fuera); deberá ver las siguientes entradas en `/var/log/messages`:

```
Feb  7 01:54:14 www kernel: Packet log: input DENY eth0
PROTO=6 129.27.43.9:1427 195.58.178.210:23 L=60 S=0x00
I=36981 F=0x4000 T=59 SYN (#119)
```

Configuración con YaST

La configuración gráfica con YaST se realiza en el Centro de Control de YaST. Una vez allí, seleccione el apartado 'Firewall' del menú 'Seguridad y Usuarios'. La configuración está dividida en cuatro secciones:

Configuración básica Defina aquí las interfaces que quiere proteger. Si se trata de un único ordenador o una red interna, introduzca la interfaz dirigida hacia el exterior (hacia Internet). Si detrás de su sistema se encuentra una red interna, ha de introducir también la interfaz dirigida hacia dentro. Salga de este diálogo con 'Siguiente'.

Servicios Esta opción sólo es relevante en caso de que, a través de su sistema, quiera ofrecer servicios que estén disponibles desde Internet (servidor web, servidor de correo, etc.). Active las casillas de control correspondientes y/o pulse el botón 'Experto ...' para activar determinados servicios a través de su número de puerto (puede consultarse en `/etc/services`). Si su máquina no va a actuar como servidor, salga de este diálogo sin efectuar ningún cambio con 'Siguiente'.

Características Seleccione aquí las características principales de su cortafuegos:

- ‘Permitir traceroute’ ayuda a comprobar el enrutamiento a su cortafuegos.
- ‘Tráfico reenviado y enmascaramiento’ protege a los ordenadores de la red local frente a Internet. Parecerá que es su cortafuegos el que utiliza todos los servicios de Internet mientras que los ordenadores internos permanecen invisibles.
- ‘Proteger todos los servicios en ejecución’ significa que se evitan todos los accesos de la red a servicios TCP y UDP del cortafuegos, exceptuando aquellos activados explícitamente en el paso anterior.
- ‘Proteger desde la red interna’ Sólo los servicios activados del cortafuegos estarán disponibles para los ordenadores *internos*. Debido a que aquí no es posible activar ningún servicio, es mejor desactivar esta opción si quiere permitir accesos desde la red local.

Una vez completada la configuración de las características, abandone este diálogo con ‘Siguiente’.

Opciones de logging Aquí puede definir el alcance del registro de su cortafuegos. Antes de activar las ‘Opciones de depuración’, tenga en cuenta que los ficheros de registro producen una gran cantidad de datos. Con la configuración del registro o logging concluye la configuración del cortafuegos. Salga de este diálogo con ‘Siguiente’ y confirme el mensaje que aparece a continuación para activar el cortafuegos.

SSH – secure shell, la alternativa segura

El trabajo en red requiere en ocasiones el acceso a sistemas remotos. En estos casos, el usuario suele tener que autenticarse con su nombre de usuario y contraseña. Si estos datos se envían en texto plano y sin codificar, cabe la posibilidad de que sean interceptados por terceros que podrían utilizarlos en su propio interés para, por ejemplo, usar la conexión del usuario sin su conocimiento. Además de poder ver todos los datos privados del usuario, el atacante podría intentar obtener derechos de administrador sobre el sistema o también utilizar la conexión recién adquirida para desde allí atacar a otros sistemas. Antiguamente se utilizaba Telnet para establecer conexiones entre dos ordenadores remotos. No obstante, este método no utilizaba ningún mecanismo de codificación o seguridad para prevenir “filtraciones”. Las conexiones de copia o FTP entre ordenadores remotos tampoco ofrecen ninguna protección.

El software SSH sí ofrece la protección necesaria. La autenticación completa, compuesta generalmente por nombre de usuario y contraseña, así como las comunicaciones se realizan aquí de forma codificada. Si bien es cierto que aún así es posible que se intercepten los datos transmitidos, estos no podrían ser leídos porque están codificados. De esta manera es posible comunicarse de forma segura a través de redes inseguras como Internet. SuSE Linux incluye con este fin el paquete OpenSSH.

El paquete OpenSSH

En SuSE Linux, el paquete OpenSSH está incluido en la instalación estándar, por lo que dispondrá de los programas `ssh`, `scp` y `sftp` como alternativa a `telnet`, `rlogin`, `rsh`, `rcp` y `ftp`.

El programa ssh

El programa `ssh` permite conectarse a un sistema de forma remota y trabajar con él interactivamente. Por este motivo constituye un sustituto tanto de `telnet` como `rlogin`. Por razones de parentesco con `rlogin`, el enlace simbólico adicional de nombre `slogin` apunta igualmente a `ssh`. Por ejemplo, con el comando `ssh sol` podremos registrarnos en el ordenador `sol`. A continuación de haber introducido el comando, el sistema preguntará la contraseña.

Después de haber conseguido una autenticación válida se podrá trabajar tanto desde la línea de comando p. ej. con el comando `ls` como de forma interactiva, p. ej. con `YAST`. Si quiere diferenciar el nombre de usuario local del usuario en el sistema remoto, hágalo mediante p. ej. `ssh -l juan sol` o bien con `ssh juan@sol`.

Además, `ssh` nos ofrece la posibilidad ya conocida en `rsh` de ejecutar comandos en otro sistema. En el siguiente ejemplo se ejecutará el comando `uptime` en el ordenador `sol` y se creará un directorio con el nombre `tmp`. Los resultados del programa se visualizarán en la terminal local del ordenador `tierra`.

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

Las comillas son en este caso necesarias para unir los comandos. Sólo de esta forma se ejecutará también el segundo comando en el ordenador `sol`.

scp – copiar de forma segura

Con la ayuda de scp se pueden copiar archivos a un ordenador remoto. scp es un sustituto seguro y codificado de rcp. Por ejemplo con el comando: `scp MiCarta.tex sol:` se copiará el archivo `MiCarta.tex` del ordenador `tierra` al ordenador `sol`. En el caso de que los nombres de usuarios en `tierra` y `sol` sean diferentes, en scp habrá que recurrir a escribir `nombre_usuario@nombre_ordenador`. No existe la opción `-l`.

Después de consultar la contraseña, scp comienza con la transmisión de datos e indica el avance mediante una barra formada por estrellas que crece de izquierda a derecha. Además se muestra en el lado derecho el tiempo restante para completar la transmisión (ingl. *estimated time of arrival*). La opción `-q` suprime todas las indicaciones en pantalla.

scp ofrece también la posibilidad de transferir de forma recursiva todo un directorio. El comando: `scp -r src/ sol:backup/`

copia el contenido completo del directorio `src/` incluyendo todos los subdirectorios al ordenador `sol`. El nombre de directorio `backup/` indicado detrás del nombre del ordenador (`sol:`), hace que los datos se guarden en `sol` dentro del directorio `backup`, que se crea automáticamente en caso de no existir.

Mediante la opción `-p`, scp mantiene fecha y hora de los archivos que se copian. Con `-C` se realiza una transferencia comprimida. Como ventaja el volumen de datos disminuye, pero en cambio el esfuerzo de cálculo es más elevado. Dada la potencia de cálculo de hoy en día, se puede despreciar este efecto negativo.

sftp - transmisión segura de datos

Otra posibilidad para la transferencia segura de datos es sftp, que ofrece muchos de los comandos conocidos de ftp una vez que la conexión se ha establecido. En comparación con scp, resulta más adecuado para transferir archivos cuyos nombres no se conocen.

El daemon SSH (sshd) – el lado del servidor

Para que se puedan utilizar los programas cliente ssh y scp, en segundo plano se debe ejecutar el daemon SSH que espera las conexiones en el puerto TCP/IP Port 22.

Al iniciarse por primera vez, el daemon genera tres pares de claves que constan de una parte pública y una privada. Por este motivo este mecanismo se considera un proceso basado en "public-key". Para garantizar la comunicación segura,

sólo el administrador de sistema debe tener el derecho de acceder a las claves privadas. Por eso en la configuración predeterminada los derechos sobre los archivos se configuran de forma correspondiente. El daemon de SSH utiliza localmente las claves privadas que no deben ser comunicadas a nadie.

En cambio, las partes públicas de las claves (se reconocen p. ej. por la extensión `.pub`) se comunican a todos los interlocutores en el proceso de comunicación y son por tanto legibles para todos los usuarios.

El cliente SSH inicia la conexión. El daemon SSH que se encontraba en espera y el cliente que pide una conexión intercambian datos de identificación para utilizar las mismas versiones de protocolo y para evitar la conexión a un puerto equivocado. En realidad, el que responde es un "proceso hijo" del daemon SSH inicial, por lo que es posible mantener al mismo tiempo muchas conexiones SSH.

Para la comunicación entre el cliente y el servidor SSH, OpenSSH soporta las versiones 1 y 2 del protocolo SSH. Al instalar SuSE Linux por primera vez se utiliza automáticamente la versión actual del protocolo, 2. En cambio, si prefiere conservar SSH 1 después de actualizar, siga las instrucciones descritas en `/usr/share/doc/packages/openssh/README.SuSE`. Allí también se describe cómo transformar en pocos pasos un entorno SSH 1 en un entorno SSH 2 operativo.

Con el protocolo SSH versión 1, el servidor envía su clave pública `host key` y una `server key` creada el daemon SSH nuevamente cada hora. El cliente SSH se sirve de estas dos claves para codificar ((ingl. *encrypt*)) una clave que varía de sesión en sesión (ingl. *session key*) y que se envía al servidor SSH. Además indica al servidor el tipo de cifrado (ingl. *cipher*).

El protocolo SSH versión 2 no incluye la `server key`. En su lugar utiliza un algoritmo de Diffie-Hellman para intercambiar las claves.

Para descifrar la clave de sesión es imprescindible disponer de las claves privadas de `host` y `server`, las cuales no se pueden obtener por medio de las partes públicas. Por este motivo, sólo el daemon SSH contactado es capaz de descifrar la clave de sesión mediante su clave privada (ver `man /usr/share/doc/packages/openssh/RFC.nr0ff`).

Es posible seguir esta fase de establecimiento de conexión mediante la opción de búsqueda de errores del programa cliente de SSH (opción `-v`). Por defecto se utiliza el protocolo SSH versión 2, pero sin embargo se puede forzar el protocolo SSH versión 1 con el parámetro `-1`.

Los ataques del tipo "man-in-the-middle" se evitan porque el cliente guarda en `~/.ssh/known_hosts` todas las claves públicas del `host` después de haber tomado el primer contacto. Los servidores SSH que tratan de camuflarse con el nombre y la IP de otro ordenador se descubren con una alerta. Se delatan ya

sea por una clave de host diferente a la que está guardada en `~/.ssh/known_hosts` o bien porque no pueden descifrar la clave de sesión por falta de la clave privada correcta.

Se recomienda guardar de forma externa las claves públicas y privadas del directorio `/etc/ssh/` y hacer una copia de seguridad de las mismas. Así es posible averiguar modificaciones de las claves y restaurarlas después de una nueva instalación. Esta restauración de las claves evita sobre todo que los usuarios se preocupen por el mensaje de advertencia. Una vez comprobado que se trata del servidor SSH correcto a pesar del aviso, es necesario borrar la entrada que se refiere a éste en el archivo `~/.ssh/known_hosts`.

Mecanismos de autenticación de SSH

Al final se realiza la verdadera autenticación en su forma más simple mediante la indicación de nombre de usuario y contraseña tal como se ha mencionado en los ejemplos anteriores.

El objetivo de SSH era proporcionar un nuevo software seguro pero al mismo tiempo fácil de usar. Al igual que los programas a los que pretende sustituir, `rsh` y `rlogin`, SSH también ha de ofrecer un método sencillo de autenticación que pueda emplearse fácilmente en el día a día.

SSH realiza la autenticación mediante otro juego de claves creado a petición del usuario. Para ello el paquete SSH dispone de la utilidad `ssh-keygen`. Después de introducir `ssh-keygen -t rsa` o `ssh-keygen -t dsa`, transcurre un tiempo hasta que el juego de claves está creado. A continuación el programa consulta el nombre de archivo para guardar las claves:

```
Enter file in which to save the key (/home/tux/.ssh/id_rsa):
```

Después confirmar la ubicación sugerida se pide una contraseña. Aunque el programa admite una contraseña vacía, es mejor introducir un texto de diez a treinta caracteres. Es preferible no utilizar palabras o frases demasiado sencillas o cortas. Después de introducirlo, el programa pide una confirmación. El programa indica entonces el lugar donde se guardan la clave privada y la pública; en el ejemplo concreto estos son los archivos `id_rsa` y `id_rsa.pub`.

```
Enter same passphrase again:
```

```
Your identification has been saved in /home/tux/.ssh/id_rsa.
```

```
Your public key has been saved in /home/tux/.ssh/id_rsa.pub.
```

```
The key fingerprint is:
```

```
79:c1:79:b2:e1:c8:20:c1:89:0f:99:94:a8:4e:da:e8 tux@sol
```

El comando `ssh-keygen -p -t rsa` o `ssh-keygen -p -t dsa` sirve para cambiar su contraseña. La parte pública de la clave (en nuestro ejemplo `id_rsa.pub`) se ha de copiar al ordenador remoto, guardándola allí como `~/.ssh/authorized_keys`. En el siguiente intento de conectar, SSH pregunta por la contraseña. Si esto no funciona, compruebe que la ubicación y el contenido de los archivos anteriormente mencionados son correctos.

A la larga este procedimiento es más complicado que la introducción de una contraseña. Por eso el paquete SSH incorpora otra utilidad llamada `ssh-agent` que mantiene claves privadas durante una sesión en entorno X. Para realizarlo, todo el entorno X Windows se inicia como un proceso hijo de `ssh-agent`.

Con este fin, el método más sencillo consiste en editar el archivo `.xsession`, asignando a la variable `usessh` el valor `yes` y después entrar al sistema con un gestor como p. ej. KDM o XDM. Otra posibilidad es la de iniciar el entorno gráfico mediante `ssh-agent startx`.

Ahora se puede utilizar `ssh` o `scp` como es habitual y si ha distribuido su clave pública como antes, no se le pedirá ninguna contraseña.

Al salir del ordenador es importante terminar la sesión X o bloquearla mediante un protector de pantalla con contraseña (p. ej. `xlock`).

Todas las modificaciones importantes realizadas con la implantación del protocolo SSH versión 2 también se encuentran documentadas en el archivo `/usr/share/doc/packages/openssh/README.SuSE`.

"X", autenticación remota y mecanismos de reenvío

Aparte de las mejoras en cuanto a la seguridad del sistema, `ssh` facilita también el trabajo con aplicaciones de X-Windows remotas. Al utilizar `ssh` con la opción `-X`, la variable `DISPLAY` en el ordenador remoto se configura automáticamente y todas las ventanas del X-Windows se mandan a través de la conexión `ssh` existente al ordenador cliente. Esta sencilla función evita la captura de datos por parte de terceros en caso de aplicaciones-X remotas con visualización local.

La opción `-A` traspassa el mecanismo de autenticación de `ssh-agent` al siguiente ordenador. Así se puede acceder de un ordenador a otro sin necesidad de introducir una contraseña. Es algo que sólo funciona si la clave pública se encuentra correctamente en todos los ordenadores destino.

Por razones de seguridad, los dos mecanismos están desactivados en la configuración predeterminada. No obstante, se pueden activar de forma permanente en el archivo de configuración global `/etc/ssh/ssh_config` o en el personal de cada usuario `~/.ssh/config`.

También se puede utilizar ssh para el reenvío de cualquier conexión TCP/IP. Como ejemplo se muestra el reenvío del puerto SMTP y POP3:

```
ssh -L 25:sol:25 tierra
```

En este caso, cualquier conexión a "tierra Port 25" se reenvía al puerto SMTP de sol a través del canal codificado. Es un procedimiento especialmente útil para usuarios de servidores SMTP que no disponen de SMTP-AUTH o de prestaciones POP-before-SMTP. Así, el servidor de correo "en casa" puede entregar el correo a cualquier lugar con conexión a Internet.

De forma análoga, el comando:

```
ssh -L 110:sol:110 tierra
```

reenvía todas las consultas hechas al puerto 110 (POP3) en tierra al puerto POP3 de sol.

Ambos ejemplos exigen la introducción de los comandos como superusuario root, ya que las conexiones se realizan con puertos locales privilegiados. Con la conexión SSH establecida, el correo se envía y se recibe como siempre en modo de usuario normal. En tal caso hay que configurar como Host SMTP y POP3 la máquina local localhost.

Se puede conseguir información adicional en la páginas de manual de los distintos programas y en los archivos que se encuentran dentro del directorio /usr/share/doc/packages/openssh.

Autenticación en la red — Kerberos

Aparte de los mecanismos habituales de identificación que son inherentemente inseguros, no existe ninguna forma de autenticar exactamente en una red abierta, los usuarios de un determinado ordenador. Esto quiere decir que cualquier persona puede ser capaz de falsificar su identidad y así recoger los e-mails de otra persona, acceder a los datos privados de ella o iniciar un determinado servicio. Por eso la red debe cumplir los siguientes requisitos para poder ser considerada como segura:

- Los usuarios deben acreditar su identidad para cada servicio y se debe asegurar que ningún usuario acoja la identidad de otro.
- Cada servidor en la red debe acreditar su identidad. En caso contrario un atacante puede identificarse como el servidor solicitado y capturar la información confidencial que se esté mandando a éste. Este proceso se

llama "Mutual Authentication", ya que el cliente se identifica frente al servidor y vice versa.

La autenticación codificada de Kerberos cumple los requisitos mencionados. A continuación se explica el funcionamiento básico de Kerberos. La implementación utilizada de Kerberos incorpora documentación más detallada al respecto.

Atención

Kerberos original se desarrolló en el MIT. Aparte de éste (MIT Kerberos) existen otras implementaciones de Kerberos. SuSE Linux contiene una implementación libre de Kerberos 5 llamada Heimdal Kerberos 5 KTH. Este capítulo se refiere a las propiedades generales de diferentes Kerberos, por lo que siempre se utiliza el término Kerberos salvo que se trate de propiedades específicas de Heimdal.

Atención

Terminología de Kerberos

Antes de comentar los detalles de Kerberos es importante tomar nota de los siguientes términos:

Credential Los usuarios o clientes tienen que disponer de credenciales que les autorizan a solicitar determinados servicios. Kerberos dispone de dos tipos de credenciales: Tickets y Authenticators.

Ticket Un Ticket es una credencial utilizada por un cliente para solicitar un servicio de un servidor. Contiene el nombre del servidor, el nombre del cliente, la dirección de Internet del cliente, una marca de tiempo (ingl. *timestamp*), el tiempo de vida de la credencial y una clave de sesión al azar. Todos estos datos se encriptan con la clave del servidor.

Authenticator Junto con el ticket se utiliza el autenticador (ingl. *Authenticator*) para asegurar que el cliente que presenta un ticket realmente es él que presume ser. El autenticador se genera en la estación de trabajo mediante su nombre, su dirección IP, la hora actual y se encripta con la clave de sesión solamente conocida por parte del cliente y del servidor al que se solicita el servicio. En comparación a un ticket, el autenticador sólo puede ser usado una vez. El cliente por sí mismo es capaz de crear un autenticador.

Principal Un Principal de Kerberos es una unidad única (un servicio o un cliente) al que se puede asignar un ticket. El Principal se compone de las siguientes partes:

- **Primary** – Es la primera parte que puede ser equivalente al nombre de usuario.
- **Instance** – Información opcional, describiendo el Primary. Esta cadena se separa por el símbolo ‘/’ del Primary.
- **Realm** – Realm determina el área de funcionamiento de Kerberos. Normalmente el Realm es equivalente al nombre de dominio en mayúsculas.

Mutual Authentication Al usar Kerberos, el cliente tal como el servidor pueden estar seguros sobre la autenticidad de su contraparte ya que se autentican mutuamente con una clave de sesión.

Session Key Las claves de sesión (ingl. *session key*) son claves privadas temporales, generadas por parte de Kerberos. Se utilizan para encriptar la comunicación entre cliente y servidor.

Replay Casi toda información que pasa por una red se puede interceptar, desviar o mandarla nuevamente. En el caso de Kerberos es muy peligroso si un atacante consigue interceptar la petición de servicio que contiene el ticket y el autenticador. Podría intentar mandar esta información nuevamente (“Replay”) y acoger así otra identidad. Afortunadamente Kerberos dispone de diferentes mecanismos para evitar este problema.

Server o Service “Service” (servicio) se utiliza para realizar una determinada operación en un “Server”.

¿Cómo funciona?

Kerberos se denomina frecuentemente como servicio de autenticación del tipo “Trusted Third Party”. Esto quiere decir que todos los clientes confían en Kerberos respecto a la identidad de otros ordenadores. Kerberos mantiene una base de datos con todos los usuarios y sus claves privadas.

Para que Kerberos merezca la confianza depositada en él, el servidor de autenticación y el servidor que otorga los tickets han de ejecutarse en una máquina aparte. Sólo el administrador debe tener acceso al servidor y los servicios que se ejecutan en él deben reducirse a un mínimo — ni siquiera `sshd` debe estar levantado.

Primer contacto El primer contacto con Kerberos se parece al login de cualquier sistema en red. Al introducir la contraseña, esa información tal como el nombre del sistema de otorgamiento de tickets, se envía al servidor de autenticación (Kerberos). Si este servidor reconoce la identidad, éste genera una clave de sesión al azar para el uso entre el cliente y el servidor de otorgamiento de tickets.

Ahora el servidor de autenticación genera un ticket para el servidor de otorgamiento de tickets que se compone de los siguientes elementos (toda información se encripta con una clave de sesión solamente conocida por parte de los servidores de autenticación y de otorgamiento de tickets):

- los nombres de los clientes y del servidor de otorgamiento de tickets
- la hora actual
- el tiempo de vida del ticket
- la dirección IP del cliente
- la clave de sesión nueva

Ahora el ticket se envía – junto con la clave de sesión – de forma codificada al cliente, pero en esta ocasión utilizando la clave privada del cliente. Solo el cliente y Kerberos conocen esta clave, ya que fue generada a partir de la contraseña de usuario. Cuando el cliente recibe esta información, el usuario tiene que introducir la contraseña. Esta contraseña se convierte en la clave que es capaz de descifrar la información que fue enviada del servidor de autenticación. Después de descifrar, la contraseña y la clave se borran de la memoria de la estación de trabajo; ésta es capaz de identificarse correctamente hasta que el tiempo de vida del ticket otorgado expire.

Solicitud de un servicio Para pedir un servicio de cualquier servidor en la red, la aplicación del cliente tiene que compulsar su identidad. Por eso la aplicación genera un identificador (ingl. *Authenticator*) que se compone de las siguientes partes:

- el Principal del cliente
- la dirección IP del cliente
- la hora actual

Toda esa información se encripta con la clave de sesión que ya recibió el cliente particularmente para ese servidor. El identificador y el ticket para el servidor se mandan a éste. El servidor por su parte utiliza su copia de la clave de sesión para decodificar el identificador que le permite obtener

toda la información necesaria del cliente que solicita el servicio. Esta información se compara con la del ticket. De esta forma el servidor comprueba si el ticket y el identificador proceden del mismo cliente.

Si por parte del servidor no existieran medidas de seguridad, este punto sería ideal para un ataque de repetición (ingl. *replay*). El agresor puede intentar enviar nuevamente una solicitud de servicio que haya sido capturada anteriormente en la red. Para evitar este tipo de ataque, el servidor no acepta ningún paquete que se envía con una marca de tiempo y un ticket ya recibidos. Además es posible rechazar peticiones de servicio cuya marca de tiempo difiere demasiado del tiempo actual (hacia el futuro o hacia el pasado).

Autenticación mutua Es posible realizar la autenticación de Kerberos en ambas direcciones. No sólo se trata del cliente que se identifica frente al servidor, el servidor también debe identificarse frente al cliente que solicita un cierto servicio. Por eso el servidor envía también un cierto identificador. Este se forma sumando 1 a la suma de control que fue recibida del cliente y el resultado se encripta con la clave de sesión compartida con el cliente. Para el cliente esta respuesta es la compulsa de la autenticidad del servidor y el trabajo entre cliente y servidor puede comenzar.

Ticket-Granting — Contactar con todos los servidores Los tickets están pensados para el uso con un solo servidor por lo que hace falta un nuevo ticket para cada servicio adicional que se solicite. Kerberos implementa un mecanismo para obtener tickets de los diferentes servidores que se denomina "Ticket Granting Service" (Servicio de expedición de tickets). Este servicio también está sometido a los protocolos de acceso ya explicados. Siempre que una aplicación necesita un ticket que aún no se haya otorgado, ésta contacta el servidor de otorgamiento de tickets. La solicitud de un ticket se compone de las siguientes partes:

- El Principal solicitado
- El ticket para el otorgamiento de ticket
- El identificador (authenticator)

Igual como los otros servidores, el servidor de otorgamiento de tickets controla el ticket recibido y el identificador. En caso de confirmar la autenticidad de ellos, el servidor de otorgamiento de tickets genera una clave de sesión nueva que se debe utilizar para la conexión del cliente con el servidor nuevo. El siguiente paso es la creación de un ticket para el servidor nuevo con la información siguiente:

- El Principal del cliente

- El Principal del servidor
- La hora actual
- La IP del cliente
- La clave de sesión recién creada

El tiempo de validez del ticket nuevo equivale al tiempo de vida restante del ticket del sistema de otorgamiento de tickets o a un valor predeterminado para este servicio, dependiendo de cuál es el tiempo inferior. El sistema de otorgamiento de tickets envía este ticket junto a una clave de sesión al cliente. En esta ocasión la respuesta es codificada con la clave de sesión que se recibió junto con el ticket original del sistema de otorgamiento de tickets. Ahora el cliente es capaz de descifrar la respuesta de un servicio nuevo que se solicite sin necesidad de pedir la contraseña de usuario nuevamente. Esta es la forma de Kerberos de conseguir tickets para el cliente, "molestando" al usuario una sola vez con la introducción de la contraseña.

Compatibilidad con Windows 2000 Windows 2000 incorpora una implementación de Kerberos 5 realizada por Microsoft. SuSE Linux utiliza la implementación Heimdal de Kerberos 5 que incorpora mucha documentación útil sobre el tema; ver [Información adicional sobre Kerberos](#) en la página siguiente.

Efectos de Kerberos a nivel de usuario

En el caso óptimo, el usuario sólo tiene contacto con Kerberos en el momento de efectuar el login en su estación de trabajo. En ese momento el cliente recibe un ticket para el otorgamiento de subsiguientes tickets. Cuando el usuario sale del sistema (logout), los tickets de Kerberos automáticamente se borran para evitar que otros usuarios puedan identificarse como otro usuario cuando no esté trabajando. Existe un conflicto cuando la sesión de trabajo del usuario dure más tiempo que el tiempo de vida máximo del ticket "maestro" para el otorgamiento de tickets (10 horas suele ser un valor razonable). Para conseguir un ticket maestro nuevo, el usuario puede iniciar kinit. No hace falta más que introducir la contraseña nuevamente y Kerberos se encarga de gestionar el acceso a todos los servicios. Mediante klist es posible obtener una lista de todos los tickets que Kerberos obtiene trabajando en segundo plano.

Todas las aplicaciones que figuran a continuación utilizan el mecanismo de autenticación de Kerberos y se encuentran en `/usr/lib/heimdal/bin`. Ofrecen la misma funcionalidad de sus homólogos de Unix/Linux a la que se añade la ventaja de la autenticación transparente mediante Kerberos:

- telnet/telnetd
- rlogin
- rsh, rcp, rshd
- popper/push
- ftp/ftpd
- su
- imapd
- pine

No hace falta introducir ninguna contraseña para utilizar estas utilidades, porque Kerberos ya realizó la identificación. Al compilar ssh con soporte de Kerberos, ssh es capaz de traspasar todos los tickets obtenidos para una determinada estación de trabajo a otra. Después de realizar un login en otra estación de trabajo, ssh se encarga de adaptar el contenido codificado de los tickets a la situación nueva. No alcanza a copiar sencillamente los tickets de una máquina a la otra, ya que contienen información específica sobre la estación de trabajo (la dirección IP). XDM y KDM también ofrecen soporte de Kerberos. La guía *Kerberos V5 UNIX User's Guide* en http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.5/doc/user-guide_toc.html ofrece información adicional sobre las utilidades de red de Kerberos.

Información adicional sobre Kerberos

SuSE Linux incorpora una implementación libre de Kerberos, denominada Heimdahl. La documentación correspondiente se encuentra en `/usr/share/doc/packages/heimdal/doc/heimdal.info` después de haber instalado el paquete `heimhah1`. Todo el proyecto está documentado en Internet bajo la dirección <http://www.pdc.kth.se/heimdal/>.

La página web oficial de la implementación de Kerberos del MIT reúne enlaces a otras fuentes interesantes:

<http://web.mit.edu/kerberos/www/>

En la siguiente dirección se encuentra un diálogo clásico que explica el funcionamiento de Kerberos. No es demasiado técnico y justo por eso es muy interesante:

<http://web.mit.edu/kerberos/www/dialogue.html>

Otra fuente de información que explica el funcionamiento básico de Kerberos y que tiene diversas citas para seguir estudiando el tema, se encuentra en:
<ftp://athena-dist.mit.edu/pub/kerberos/doc/usenix.PS>

Los siguientes enlaces ofrecen una introducción breve a Kerberos y responden a muchas preguntas en torno a la instalación, configuración y administración:

http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.5/doc/user-guide_toc.html

http://www.lns.cornell.edu/public/COMP/krb5/install/install_toc.html

http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.5/doc/admin_toc.html

Las FAQ oficial de Kerberos se encuentran en:

<http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html>

Tung, Brian: *Kerberos — A Network Authentication System*. Addison Wesley, 1999.

- (ISBN 0-201-37924-4)

Instalación y administración de Kerberos

Esta sección trata los aspectos relacionados con la instalación de Heimdal Kerberos así como algunas cuestiones de administración. El texto asume que está familiarizado con los conceptos básicos de Kerberos (si desea obtener más información a este respecto, consulte la sección *Autenticación en la red — Kerberos* en la página 508).

Elección de Realms en Kerberos

El “dominio” de una instalación Kerberos se denomina Realm y se identifica por su nombre, como por ejemplo, FOOBAR.COM o simplemente CONTABILIDAD. Kerberos distingue entre letras mayúsculas y minúsculas, por lo que foobar.com es un realm diferente a FOOBAR.COM. Utilizar mayúsculas o minúsculas es una cuestión de preferencias. Sin embargo, es una práctica común reservar las letras mayúsculas para los nombres de los realm.

Se recomienda utilizar el nombre de dominio DNS (o un subdominio, tal como CONTABILIDAD.FOOBAR.COM). Como se explica a continuación, la labor de un administrador puede ser mucho más sencilla si configura los clientes Kerberos para localizar el KDC y otros servicios Kerberos a través de DNS. Para lograr este objetivo, resulta bastante útil que el realm sea un subdominio del nombre de dominio DNS.

A diferencia del espacio de nombres DNS, Kerberos no dispone de una estructura jerárquica. No puede configurarse un realm denominado `FOOBAR.COM`, disponer dos "subrealms" llamados `DESARROLLO` y `CONTABILIDAD` bajo él y esperar que los dos realms subordinados hereden de alguna forma los principales de `FOOBAR.COM`. En su lugar, es necesario establecer tres realms independientes, para los cuales será necesario configurar la autenticación "crossrealm" a fin de que los usuarios de un realm puedan interactuar con los servidores o usuarios de otro.

Con el fin de lograr una mayor simplicidad, se asume que se está configurando sólo un realm para dar servicio a toda la organización. Existen algunos documentos, tales como `?`, que detallan cómo configurar la autenticación crossrealm. Durante el resto de esta sección, se utiliza el nombre de realm `SAMPLE.COM` para todos los ejemplos.

Configuración del hardware KDC

El primer paso que ha de dar cuando se desea utilizar Kerberos es configurar un equipo que asuma el papel de centro de distribución de claves o KDC (Key Distribution Center). Esta máquina albergará la base de datos completa de usuarios Kerberos con sus contraseñas y el resto de información relacionada.

El KDC es el elemento más importante dentro de su infraestructura de seguridad; si alguien consigue acceder a él, todas las cuentas de usuario y toda la estructura protegida por Kerberos estará comprometida. Un atacante con acceso a la base de datos Kerberos puede suplantar a cualquier principal de la base de datos. Asegúrese de que extrema la seguridad alrededor de este equipo tanto como le sea posible:

- Coloque el servidor en un lugar físicamente seguro, como por ejemplo una sala de servidores cerrada bajo llave a la cual sólo pueda acceder un reducido número de personas.
- No ejecute ninguna aplicación de red en él a excepción de KDC. Esto incluye servidores y clientes; por ejemplo, el KDC no debe poder importar ningún sistema de archivos a través de NFS o utilizar DHCP para cargar su configuración de red.

Una de las estrategias que puede seguir para conseguir maximizar la seguridad es realizar, en primer lugar, una instalación mínima del sistema, comprobar la lista de paquetes instalados y eliminar todos aquellos que resulten innecesarios. Esto incluye servidores, tales como `inetd`, `portmap` y cups así como cualquiera que esté basado en X11.

Incluso la instalación de un servidor SSH puede suponer un riesgo potencial para la seguridad.

Por razones también de seguridad, no se proporciona ningún acceso en modo gráfico para este equipo mediante un servidor X. Kerberos dispone de su propia interfaz de administración.

- Configure `/etc/nsswitch.conf` a fin de que sólo se utilicen archivos locales para la búsqueda de usuarios y grupos. Modifique las líneas de `passwd` y `group` de la siguiente forma:

```
passwd:      files
group:       files
```

Edite los archivos `passwd`, `group`, `shadow` y `gshadow` en `/etc` y elimine las líneas que comienzan con el carácter `+` (destinadas a las búsquedas NIS).

Asimismo, considere la deshabilitación de las búsquedas DNS, ya que existe un riesgo potencial relacionado con ellas. Si existe algún fallo de seguridad en la librería del componente DNS, un atacante podría engañar al KDC para que realizara una petición DNS que activara el fallo. Para desactivar las búsquedas DNS, simplemente ha de eliminar `/etc/resolv.conf`.

- Deshabilite todas las cuentas de usuario excepto la de `root` mediante la modificación de `/etc/shadow` y reemplace las contraseñas enmascaradas con caracteres `* o !`.

Sincronización del reloj

Para poder utilizar Kerberos con éxito, asegúrese de que todos los relojes de los sistemas pertenecientes a la organización están sincronizados dentro de un cierto rango. La razón de ser de esta medida reside en que Kerberos intentará protegerle de las credenciales "dobladadas". Un atacante podría observar las credenciales Kerberos en la red y reutilizarlas para atacar al servidor. Kerberos emplea una serie de tácticas defensivas para evitar esto. Una de ellas consiste en identificar mediante la fecha y la hora sus tickets. Si un servidor recibe un ticket con una fecha y hora que no son las actuales, lo rechazará.

Por supuesto, Kerberos permite un cierto margen cuando realiza estas comparaciones. Sin embargo, los relojes de los equipos pueden llegar a ser muy inexactos en mantener la hora correcta (no es infrecuente escuchar como algunos relojes de PC pueden llegar a retrasarse o adelantarse hasta media hora durante el

transcurso de una semana). Por tanto, es necesario configurar todos los equipos pertenecientes a la red para que sincronicen sus relojes respecto a una fuente horaria central.

Un método sencillo para lograr este objetivo es instalar un servidor horario NTP en uno de los equipos e indicar a todos los clientes que sincronicen sus relojes respecto a éste. Este proceso puede llevarse a cabo mediante la ejecución de un daemon NTP en modo cliente en todos los equipos o ejecutando el comando `ntpdate` una vez al día desde todas las estaciones de trabajo (esta solución sólo es apropiada si se trata de un número reducido de sistemas).

El propio KDC también necesita estar sincronizado respecto a la fuente horaria común. Debido al riesgo en la seguridad que podría producirse si ejecutara él mismo un daemon NTP, se recomienda ejecutar un comando `ntpdate` como una entrada cron.

La configuración de un servidor NTP no entra dentro del alcance de esta sección. Si necesita recabar más información al respecto, consulte la documentación sobre NTP incluida en el sistema instalado en el archivo `/usr/share/doc/packages/xntp-doc`.

Por supuesto, también puede adaptar a sus necesidades la diferencia máxima tolerada por Kerberos al comprobar las marcas de tiempo o *time stamps*. Es posible modificar este valor (`clock skew`) en el archivo de configuración `krb5.conf` como se describe en la sección [Adaptar la diferencia del reloj](#) en la página 524.

Configuración del registro

Por defecto, los daemons Kerberos que se ejecutan en el equipo KDC registran la información mediante el daemon `syslog`. Si desea monitorizar qué está haciendo el KDC, puede procesar los archivos de registro de forma regular y buscar en ellos eventos inusuales o problemas potenciales.

Para ello, puede utilizar bien un script de escaneo de registros a través de la propia consola del KDC o copiar los archivos desde el KDC a otro equipo a través de `rsync` y llevar a cabo el análisis allí. No se recomienda el reenvío de los registros mediante los mecanismos incluidos en `syslog` ya que la información atraviesa la red de forma no codificada.

Instalación del KDC

Esta sección se centra en la instalación inicial del KDC, incluyendo la creación de un principal administrativo.

Instalación de los RPMs

Antes de comenzar, instale el software de Kerberos. En el lado del KDC, instale los RPM `heimdal`, `heimdal-lib` y `heimdal-tools`:

```
rpm -ivh heimdal-*.rpm heimdal-lib-*.rpm heimdal-tools*.rpm
```

Definir la clave maestra

El siguiente paso consiste en iniciar la base de datos en la que Kerberos almacena toda la información sobre los principales. En primer lugar, establezca la clave maestra de la base de datos, la cual se utiliza para proteger ésta de una exposición accidental, especialmente cuando se realiza una copia de seguridad de ella en una cinta.

La clave maestra se deriva de una frase de paso (contraseña formada por varias palabras) y se guarda en un archivo denominado "escondite" (stash file). De esta forma se consigue que no sea necesario escribir la contraseña cada vez que se reinicializa el KDC. Asegúrese de escoger una buena frase de paso, como por ejemplo una procedente de un libro abierto por una página al azar.

Cuando realiza copias de seguridad de la base de datos Kerberos (`/var/heimdal/heimdal.db`), no copie el archivo escondite (que reside en `/var/heimdal/m-key`). En caso contrario, aquellas personas que tuvieran acceso a la cinta podrían también descifrar la base de datos. Por tanto se recomienda guardar una copia de la frase de paso en un lugar seguro y diferente, ya que será necesario utilizarla si ha de restaurar la base de datos desde una copia de seguridad.

Para determinar la clave maestra, ejecute la utilidad `kstash` sin ningún argumento e introduzca la frase de paso dos veces:

```
kstash
```

```
Master key:<enter pass phrase>
```

```
Verifying password - Master key:<enter pass phrase again>
```

Creación del realm

Finalmente, cree las entradas para el realm en la base de datos Kerberos. Invoque la utilidad `kadmin` con la opción `-l` tal y como se muestra a continuación. Este argumento indica a `kadmin` que acceda a la base de datos de forma local. Por defecto, intentará contactar con el servicio `admin` de Kerberos a través de la red. En ese momento esta conexión no podrá llevarse a cabo ya que el servicio aún no se estará ejecutando.

A continuación, ordene a `kadmin` que inicie el realm. Se le solicitará que conteste a una serie de preguntas. Le recomendamos que acepte las respuestas que sugiere inicialmente `kadmin`:

```
kadmin -l
```

```
kadmin> init SAMPLE.COM
Realm max ticket life [unlimited]: <press return>
Realm max renewable ticket life [unlimited]: <press return>
```

A fin de verificar que se ha completado el proceso, utilice el comando `list`:

```
kadmin> list *
default@SAMPLE.COM
kadmin/admin@SAMPLE.COM
kadmin/hprop@SAMPLE.COM
kadmin/angepw@SAMPLE.COM
krbtgt/SAMPLE.COM@SAMPLE.COM
angepw/kerberos@SAMPLE.COM
```

Esta acción muestra que ya existe una serie de principales en la base de datos. Todos ellos son utilizados por Kerberos para procesos internos.

Creación de un principal

A continuación, cree dos principales Kerberos para usted: un principal "normal" para el trabajo del día a día y uno para tareas administrativas relacionadas con Kerberos. Asumiendo que su nombre de usuario es `newbie`, siga los siguientes pasos:

```
kadmin -l
```

```
kadmin> add newbie
Max ticket life [1 day]: <press return>
Max renewable life [1 week]: <press return>
Principal expiration time [never]: <press return>
Password expiration time [never]: <press return>
Attributes []: <press return>
newbie@SAMPLE.COM's Password: <type password here>
Verifying password: <re-type password here>
```

Acepte los valores por defecto pulsando **Intro**. Elija una buena contraseña.

Seguidamente, cree otro principal denominado `newbie/admin` mediante la instrucción `add newbie/admin` en la línea de comandos de `kadmin`. El texto

admin añadido al nombre de usuario es lo que se denomina "rol" (ingl. *role*). Este rol administrativo se utiliza posteriormente para gestionar la base de datos de Kerberos.

Un usuario puede tener distintos "roles" para cumplir diferentes propósitos. Su manejo es semejante al de cuentas de usuario totalmente distintas pero con nombres parecidos.

Inicio del KDC

Arranque los daemons KDC. Éstos incluyen el propio kdc (el daemon que gestiona la autenticación de usuario y peticiones de ticket), kadmind (el servidor que lleva a cabo la administración remota) y kpasswd (que tiene como misión manejar los aspectos relacionados con las peticiones de modificación de contraseña). Para iniciar el daemon de forma manual, escriba:

```
rckdc start
```

```
Starting kdc                done
```

Asimismo, asegúrese de que el KDC arranca por defecto cuando se reinicia el servidor. Para ello puede utilizar el comando `insserv kdc`.

Configuración de los clientes Kerberos

Cuando se configura Kerberos, existen básicamente dos estrategias que pueden seguirse: una configuración estática a través del archivo `/etc/krb5.conf` o una dinámica mediante DNS. Si se utiliza esta última, las aplicaciones Kerberos intentarán localizar los servicios KDC a través de los registros DNS. Con una configuración estática, es necesario añadir los nombres de host del servidor KDC a `krb5.conf` (y actualizar el archivo siempre que mueva el KDC o reconfigure el realm de alguna forma).

La configuración basada en DNS es, normalmente, mucho más flexible, siendo la cantidad de trabajo necesaria para configurar cada uno de los equipos mucho menor. Sin embargo, requiere que el nombre del realm sea bien el mismo que el correspondiente al dominio DNS o bien un subdominio de él.

La configuración de Kerberos vía DNS genera, por otro lado, un contratiempo relacionado con la seguridad, que consiste en que un atacante puede desestabilizar seriamente la infraestructura a través de DNS (por ejemplo, cerrando el servidor de nombres, alterando los registros DNS, etc). En cualquier caso esto significa que, como mucho, pueda producirse un ataque por denegación de servicio. Un escenario similar puede aplicarse en el caso de una configuración estática a no ser que se introduzcan únicamente direcciones IP dentro del archivo `krb5.conf` en lugar de nombres de host.

Configuración estática

labelsec:kerbadm.in.client.stat

Una forma de configurar Kerberos consiste en modificar el archivo de configuración `/etc/krb5.conf`. Este archivo, que está incluido por defecto en el sistema instalado, contiene varias entradas de muestra. Elimínalas antes de empezar a realizar su propia configuración:

`krb5.conf` está compuesto de varias secciones, cada una de las cuales comienza con su nombre entre corchetes (`[nombre]`).

Para la configuración estática, añade las siguientes líneas al archivo `krb5.conf` (donde `kdc.sample.com` es el nombre de host del KDC):

```
[libdefaults]
    default_realm = SAMPLE.COM

[realms]
    SAMPLE.COM = {
        kdc = kdc.sample.com
        kpasswd_server = kdc.sample.com
        admin_server = kdc.sample.com
    }
```

Sobre la línea `default_realm` se define el realm estándar para las aplicaciones Kerberos.

Si dispone de varios realms, simplemente añade otra instrucción a la sección `[realms]`.

Adicionalmente, añade una línea a este archivo que indique a las aplicaciones cómo mapear los nombres de host a un realm. Por ejemplo, cuando se establece una conexión a un host remoto, la librería Kerberos necesita conocer en qué realm está localizado este host. Este extremo ha de ser configurado en la sección `[domain_realms]`:

```
[domain_realm]
    .sample.com = SAMPLE.COM
    www.foobar.com = SAMPLE.COM
```

El ejemplo anterior comunica a la librería que todos los hosts en los dominios DNS `sample.com` están ubicados en el realm Kerberos `SAMPLE.COM`. Asimismo, un host externo denominado `www.foobar.com` puede ser también considerado como un miembro del realm `SAMPLE.COM`.

Configuración basada en DNS

La configuración Kerberos basada en DNS utiliza en gran medida los registros SRV (consulte el documento (RFC2052) *A DNS RR for specifying the location of services* ubicado en la dirección <http://www.ietf.org>). Estos registros no están soportados en las anteriores implementaciones del servidor de nombres BIND. Como mínimo, se requiere la versión 8 de BIND.

En lo que concierne a Kerberos, el nombre de un registro SRV tiene una estructura equivalente a `_service._proto.realm`, donde `realm` es el realm Kerberos. Recuerde que los nombres de dominio en DNS no distinguen entre mayúsculas y minúsculas, por lo que los realms de Kerberos, que sí que las distinguen, tienen problemas cuando se utiliza este método de configuración. `_service` es un nombre de servicio (se utilizan nombres diferentes cuando se intenta contactar con el KDC o el servicio de contraseñas, por ejemplo). `_proto` puede ser bien `_udp` o `_tcp`, pero no todos los servicios soportan ambos protocolos.

La parte de datos en los registros de un recurso SRV consiste en un valor de prioridad, un peso, un número de puerto y un nombre de host. La prioridad define el orden por el cual debe intentarse la conexión a los hosts (un valor menor indica una prioridad mayor). El peso se utiliza para soportar un cierto tipo de balanceo de carga entre servidores que disponen de igual prioridad. Es probable que nunca necesite modificar este argumento, así que puede mantenerlo como cero.

En la actualidad, Heimdal Kerberos examina los siguientes nombres cuando intenta buscar servicios:

_kerberos Define la ubicación del daemon KDC (el servidor que gestiona la autenticación y asigna los tickets). Los registros típicos poseen el siguiente formato:

```
_kerberos._udp.SAMPLE.COM. IN SRV 0 0 88 kdc.sample.com.
_kerberos._tcp.SAMPLE.COM. IN SRV 0 0 88 kdc.sample.com.
```

_kpasswd Describe la localización del servidor encargado de atender a las peticiones de modificación de contraseña. El aspecto habitual de estos registros se muestra a continuación:

```
_kpasswd._udp.SAMPLE.COM. IN SRV 0 0 464 kdc.sample.com.
```

Debido a que `kpasswd` no soporta TCP, no debería existir ningún registro `_tcp`.

_kerberos-adm Informa de la ubicación del servicio de administración remota. La forma usual de estas entradas es la siguiente:

```
_kerberos-adm._tcp.SAMPLE.COM. IN SRV 0 0 749 kdc.sample.com.
```

Ya que kadmind no proporciona soporte para UDP, no debería mostrarse ningún registro `_udp`.

Al igual que sucede con el archivo de configuración estática, existe un mecanismo para informar a los clientes que un host específico pertenece al realm `SAMPLE.COM`, aún cuando no forme parte del dominio DNS `sample.com` DNS. Para ello, se añade un registro TXT a `_kerberos.hostname`, tal y como se muestra a continuación:

```
_kerberos.www.foobar.com. IN TXT "SAMPLE.COM"
```

Adaptar la diferencia del reloj

Mediante la variable `clock skew` es posible definir los límites de tolerancia dentro de los cuales se aceptará un ticket cuya hora no coincida exactamente con la que muestre el reloj del sistema servidor.

Por regla general, este límite es de 300 segundos (5 minutos). Es decir, un ticket puede tener una marca de tiempo 5 minutos adelantada o atrasada con respecto a la hora del sistema del servidor y todavía será aceptado.

Si utiliza NTP para sincronizar los relojes de todos los hosts, este valor puede reducirse a un minuto.

Modifique la variable `clock skew` en `/etc/krb5.conf` como se muestra a continuación:

```
[libdefaults]
    clockskew = 120
```

Configuración de la administración remota

Para añadir o eliminar principales de la base de datos Kerberos sin tener acceso directo a la consola del KDC, comunique al servidor de administración de Kerberos cuáles son los principales autorizados.

Para ello puede editar el archivo `/var/heimdal/kadmind.acl` (ACL es la abreviatura de Access Control List o listas de control de acceso). El archivo ACL permite definir los privilegios y la configuración detallada del grado de control. Puede obtener más información en la página del manual `man 8 kadmind`.

Para autorizarse a llevar a cabo todas las acciones que Vd. quiera en la base de datos, añada la siguiente línea al archivo:

`newbie/admin``all`

Sustituya `newbie` por su nombre de usuario y reinicie KDC para aplicar los cambios.

Administración remota con `kadmin`

Llegado este punto ya será posible administrar Kerberos de forma remota con ayuda de la herramienta `kadmin`. En primer lugar, necesita obtener un ticket para el principal administrativo y a continuación emplearlo en la conexión al servidor `kadmin`:

```
kinit newbie/admin
```

```
newbie/admin@SAMPLE.COM's Password: <enter password>
```

```
/usr/sbin/kadmin
```

```
kadmin> privs  
change-password, list, delete, modify, add, get
```

Para verificar de qué privilegios dispone, puede utilizar el comando `privs`. La lista mostrada previamente presenta el conjunto completo de privilegios.

A modo de ejemplo, puede modificar el principal `newbie`:

```
kadmin> mod newbie  
Max ticket life [1 day]:2 days  
Max renewable life [1 week]:  
Principal expiration time [never]:2003-01-01  
Password expiration time [never]:  
Attributes []:
```

Esta acción modifica la vida máxima del ticket a dos días y establece la fecha de caducidad de la cuenta para el 1 de enero de 2003.

Comandos básicos de `kadmin`

A continuación se incluye una lista de los comandos más importantes de `kadmin`. Consulte página del manual de `kadmin` (`man 8 kadmin`) para obtener información más detallada.

add *<principal>* añade un nuevo principal

modify *<principal>* edita varios atributos de un principal, tales como la vida máxima del ticket y la fecha de caducidad de la cuenta

delete *<principal>* elimina un principal de la base de datos

rename *<principal>* *<newname>* renombra un principal a *<newname>*

list *<pattern>* visualiza una lista con todos los principales que coinciden con el patrón suministrado. El mecanismo de funcionamiento de los patrones es similar al de los patrones utilizados en la shell: `list newbie*` presentaría `newbie` y `newbie/admin` en este ejemplo.

get *<principal>* visualiza una información detallada acerca del principal

passwd *<principal>* modifica la contraseña del principal

Es posible acceder en todo momento a una función de ayuda introduciendo `?` y `(Intro)`, incluso dentro de los mensajes originados por los comandos como `modify` o `add`.

La instrucción `init` utilizada cuando se crea inicialmente el realm (así como en otras escasas ocasiones) no está disponible en el modo remoto. Para crear un nuevo realm, acceda a la consola del KDC y emplee `kadmin` en modo local (indicando la opción `-l` en la línea de comandos).

Creación de principales de host en Kerberos

Cada una de las máquinas dentro de la red ha de poder contactar con un KDC y se le debe haber asignado un realm Kerberos. Además, es necesario crear un principal de host o "host principal" para cada máquina.

Hasta ahora se han tratado únicamente las credenciales de usuario. No obstante, los servicios "kerberizados" también deben autenticarse en la mayoría de los casos frente al usuario cliente. Para ello existen en la base de datos Kerberos los "host principals" para todos los hosts dentro de un realm.

La sintaxis del nombre es: `host/<nombre_host>@<REALM>`, *<nombre_host>* es aquí el nombre completo del host correspondiente.

Aunque los principales de host se asemejan en muchos aspectos a los principales normales de usuario, existen también algunas diferencias. La más importante radica en que la clave del principal de usuario está protegida por contraseña. Si el usuario obtiene un ticket de KDC para determinar la autorización, ha de introducir su contraseña para que Kerberos pueda descifrar el ticket. Por

consiguiente, para un administrador de sistemas sería muy incómodo, ya que tendría que solicitar nuevos tickets para el daemon SSH cada ocho horas.

En el caso del principal de host, el problema se resuelve de la siguiente manera: La clave necesaria para codificar el ticket original para el principal de host es solicitada una vez por el administrador de KDC. Posteriormente esta clave se guarda en un archivo llamado `keytab`. Los servicios como el daemon SSH evalúan esta clave y la utilizan para recibir automáticamente nuevas claves si fuera necesario. El archivo `keytab` estándar se encuentra en `/etc/krb5.keytab`.

Puede crear un principal de host para `machine.sample.com` introduciendo lo siguiente durante su sesión con `kadmin`:

```
kinit newbie/admin
```

```
newbie/admin@SAMPLE.COM's Password: <type password>
```

```
kadmin add -r host/machine.sample.com
```

```
Max ticket life [1 day]:
Max renewable life [1 week]:
Principal expiration time [never]:
Password expiration time [never]:
Attributes []:
```

En lugar de definir una contraseña para el nuevo principal, la opción `-r` ordena a `kadmin` generar una clave aleatoria. En este caso es posible porque no deseamos ninguna actividad de usuario para este principal. Se trata puramente de una cuenta de servidor para esta máquina.

Finalmente, extraiga la clave y guárdela en el archivo `keytab` local `/etc/krb5.keytab`. Este archivo pertenece al superusuario, por lo que debe ejecutar el siguiente comando como usuario `root`:

```
ktutil get host/machine.sample.com
```

A continuación y como se describe anteriormente, utilice el comando `kdestroy` para destruir el ticket de administración recibido a través de `kinit`.

Activación del soporte PAM para Kerberos

SuSE Linux incluye un módulo PAM denominado `pam_krb5` que ofrece soporte para el acceso y actualización de contraseña bajo Kerberos. Este módulo puede

ser utilizado por distintas aplicaciones tales como el acceso a consola, su y las aplicaciones de acceso gráfico como KDM, donde el usuario introduce la contraseña y requiere de la aplicación de autenticación la obtención de un ticket inicial Kerberos.

A partir de esta versión de SuSE Linux, el módulo `pam_unix` soporta la autenticación mediante Kerberos y los cambios de contraseñas. para activar el soporte de Kerberos en `pam_unix`, modifique el archivo `/etc/security/pam_unix2.conf` de este modo:

```
auth:      use_krb5 nullok
account:   use_krb5
password:  use_krb5 nullok
session:   none
```

Cuando este archivo se evalúe, todos los servicios utilizarán Kerberos para autenticar a los usuarios. En caso de que un usuario no disponga de un principal Kerberos, `pam_unix` utilizará el mecanismo de autenticación por contraseña. La contraseña de Kerberos debería poder actualizarse de manera transparente con el comando `passwd`.

Puede configurar `pam_krb5` realizando cambios en el archivo `/etc/krb5.conf` y también añadiendo aplicaciones estándar para `pam`. El proceso se describe con detalle en la página del manual `man 5 pam_krb5`.

El módulo `pam_krb5` **no** fue específicamente diseñado para servicios de red que aceptaran tickets Kerberos como parte de la autenticación de usuario; ésta es una historia completamente diferente que se explicará en secciones posteriores.

Configuración de SSH para la autenticación con Kerberos

OpenSSH soporta la autenticación con Kerberos tanto en la versión 1 como 2 del protocolo. La versión 1 utiliza un tipo determinado de mensajes de protocolo para transmitir los tickets de Kerberos. La versión 2 ya no emplea Kerberos directamente sino "GSSAPI", *General Security Services API*. Esta interfaz de programación no es específica para Kerberos, sino que fue desarrollada para ocultar las características del sistema de autenticación subyacente de la aplicación, independientemente de que sea Kerberos, SPKM u otro sistema semejante. No obstante, la actual librería GSSAPI de SuSE Linux sólo soporta Kerberos.

Para utilizar `sshd` con la autenticación Kerberos, edite `/etc/ssh/sshd_config` y defina las opciones siguientes:

```
# These are for protocol version 1
KerberosAuthentication yes
KerberosTgtPassing yes
# These are for version 2
GSSAPIAuthentication yes
GSSAPIKeyExchange yes
```

A continuación, reinicie el daemon SSH con la instrucción `rcsshd restart`.

Si quiere utilizar la autenticación con Kerberos con la versión 2 del protocolo, ha de activar el soporte correspondiente también en el lado del cliente. Esto puede hacerse bien para todo el sistema mediante el archivo de configuración `/etc/ssh/ssh_config` o bien en base a usuarios a través del archivo `~/.ssh/config`. En ambos casos se debe añadir la opción `GSSAPIAuthentication yes` al archivo de configuración.

En este momento debería poderse conectar mediante autenticación Kerberos. Utilice `klist` para comprobar si dispone de un ticket válido para establecer una conexión con el servidor SSH. Para forzar la utilización de la versión 1 del protocolo SSH, introduzca la opción `-1` en la línea de comandos.

```
ssh earth.sample.com
```

```
Last login: Fri Aug  9 14:12:50 2002 from zamboni.sample.com
Have a lot of fun...
```

Utilización de LDAP y Kerberos

Con el uso de Kerberos, LDAP permite distribuir información de usuarios (número de identificación de usuario, grupos, directorios locales, etc.) en la red local. Ni que decir tiene que esto exige medidas de codificación muy severas para evitar, por ejemplo, la falsificación de paquetes.

Kerberos puede también utilizarse para la comunicación LDAP.

OpenLDAP implementa la mayoría de los tipos de autenticación a través de SASL, *Simple Authentication Session Layer*. SASL es básicamente un protocolo de red usado para la autenticación. SuSE Linux utiliza la implementación `cyrus-sasl` y soporta distintos tipos de autenticación. La autenticación con Kerberos se implementa vía GSSAPI (General Security Services API).

El plugin SASL para GSSAPI no está incluido en la instalación estándar. Puede instalarlo manualmente con:

```
rpm -ivh cyrus-sasl-gssapi-*.rpm
```

Para poder enlazar Kerberos con el servidor OpenLDAP, cree un principal `ldap/earth.sample.com` y añádalo a `keytab`:

```
kadmin add -r ldap/earth.sample.com
ktutil get ldap/earth.sample.com
```

En este punto ha de tener en cuenta el siguiente obstáculo: el servidor LDAP (`slapd`) funciona de manera estándar para el grupo y usuario `ldap`, mientras que `keytab` sólo puede ser leído por el usuario `root`. Por lo tanto dispone de dos opciones: cambiar la configuración de LDAP para que el servidor sea iniciado como usuario `root` u otorgar al grupo `ldap` derechos de lectura sobre `keytab`.

Para operar `slapd` como usuario `root`, edite el archivo `/etc/sysconfig/openldap` y desactive las variables `OPENLDAP_USER` y `OPENLDAP_GROUP` introduciendo un signo de comentario al principio de las líneas.

Para hacer el archivo `keytab` legible para el grupo `ldap`, cambie los derechos de este modo:

```
chgrp ldap /etc/krb5.keytab
chmod 640 /etc/krb5.keytab
```

Aunque ninguna de ambas soluciones es perfecta, actualmente no es posible configurar OpenLDAP de forma que utilice su propio archivo `keytab`.

Finalmente, reinicie el servidor LDAP con el comando `rcldap restart`.

Autentificación Kerberos con LDAP

Ahora ha de poder ejecutar aplicaciones como `ldapsearch` automáticamente con autentificación Kerberos.

```
ldapsearch -b ou=People,dc=suse,dc=de '(uid=newbie)'
```

```
SASL/GSSAPI authentication started
SASL SSF: 56
SASL installing layers
[...]
```

```
# newbie, People, suse.de
```

```
dn: uid=newbie,ou=People,dc=suse,dc=de
uid: newbie
cn: Olaf Kirch
[...]
```

Como puede ver en las líneas superiores, `ldapsearch` emite el mensaje de que ha iniciado la autenticación GSSAPI. El siguiente mensaje, algo más críptico, indica el "Security Strength Factor" (SSF) como 56. (El valor 56 en este caso es algo arbitrario. Seguramente haya sido escogido porque representa el número de bits de una clave de cifrado DES). Lo que esta línea significa realmente es que la autenticación GSSAPI ha tenido éxito y que la conexión LDAP estará protegida por codificación.

No olvide que la autenticación con Kerberos es un proceso recíproco. Es decir, no es sólo usted quien se ha autenticado de cara al servidor LDAP. Éste también se ha autenticado frente a usted. De esta forma puede estar seguro de comunicarse con el servidor LDAP previsto y no con otro servicio simulado por un agresor.

En aquellos casos donde puedan usarse distintos mecanismos SASL, puede obligar a `ldapsearch` a utilizar GSSAPI introduciendo la opción `-Y GSSAPI` en la línea de comandos.

Autenticación con Kerberos y controles de acceso LDAP

En el apartado anterior nos hemos autenticado con éxito frente al servidor LDAP. En el siguiente paso se verá cómo permitir a todos los usuarios modificar el atributo `login shell` en sus datos de usuario LDAP.

Suponiendo que utilice una estructura según la cual la entrada LDAP del usuario `joe` se encuentra en `uid=joe,ou=people,dc=suse,dc=de`, puede definir las siguientes reglas de acceso en el archivo `/etc/openldap/slapd.conf`:

```
# This is required for things to work _at all_
access to dn.base="" by * read
# Let each user change their login shell
access to dn="*,ou=people,dc=suse,dc=de" attrs=loginShell
    by self write
# Every user can read everything
access to *
    by users read
```

La segunda instrucción confiere a los usuarios autenticados derechos de escritura sobre el atributo `loginShell` de su entrada LDAP. La tercera instrucción

otorga a todos los usuarios autenticados permiso de lectura para todo el directorio LDAP.

Ahora bien, ¿cómo puede averiguar el servidor LDAP que `joe@SAMPLE.COM` de Kerberos es el equivalente de LDAP DN (ingl. *distinguished name*) `uid=joe,ou=people,dc=suse,dc=de`? Esta correspondencia se define manualmente a través de la directiva `saslExpr`. En el ejemplo se añade a `slapd.conf`:

```
saslRegexp
    uid=(. *),cn=GSSAPI,cn=auth
    uid=$1,ou=people,dc=example,dc=com
```

Para comprender este mecanismo es necesario tener en cuenta que OpenLDAP crea un DN cada vez que SASL autentifica un usuario. Este DN se compone del nombre transmitido por SASL (como p. ej. `joe`) y del tipo de autenticación SASL (GSSAPI). El resultado en este caso sería `uid=joe,cn=GSSAPI,cn=auth`.

Si se ha configurado un `saslRegexp`, el servidor LDAP comprueba el DN de la información SASL con el primer argumento como expresión regular. Si esta expresión regular resulta válida, el nombre es sustituido por el segundo argumento de la instrucción `saslRegexp`. El comodín (`$1`) es reemplazado por la parte de la expresión detectada a través de la expresión `(. *)`.

También es posible definir complicados patrones de búsqueda. Si utiliza una estructura de directorios compleja o si el nombre de usuario en la estructura que usted emplea no es parte del DN, puede usar expresiones de búsqueda que realicen la correspondencia entre el DN de SASL y el DN de usuario.

La seguridad, una cuestión de confianza

Conceptos básicos

Una de las características fundamentales de un sistema Linux/Unix es que varios usuarios (multi-user) pueden realizar en un mismo ordenador diferentes tareas al mismo tiempo (multi-tasking). Por otra parte el sistema operará en red de forma transparente, lo que significa que el usuario no podrá percibir si los datos o aplicaciones con los que se esté trabajando se encuentran alojados de forma local en el ordenador o en alguna otra parte.

Esta característica particular de que varios usuarios puedan trabajar con el sistema, exige que estos usuarios y sus datos también puedan ser diferenciados unos de otros. Dado que en este contexto intervienen otros aspectos como

pueden ser los de índole emocional, esto hace que se le dedique especial atención a la seguridad y a la protección de la privacidad.

El término protección de datos existe desde la época en que los ordenadores aún no estaban unidos entre sí mediante una red. En aquellos tiempos lo primordial era que después de una pérdida o después de un fallo en el dispositivo de almacenamiento (por lo general el disco duro) los datos siguieran estando disponibles, incluso si este fallo provocaba la caída temporal de una infraestructura mayor. Si bien este capítulo del manual de SuSE trata principalmente de la confidencialidad de los datos y de la protección de la privacidad del usuario, hay que destacar que un concepto amplio de seguridad siempre contempla que se realice un backup periódico que funcione correctamente y que sea revisado. Sin el backup de los ficheros no sólo será difícil acceder a los datos en caso de un fallo del hardware sino también particularmente cuando exista la sospecha de que alguien ha tenido acceso a ciertos datos sin disponer de autorización.

Seguridad local y seguridad en la red

Parece sensato y lógico considerar que el acceso a los datos de un ordenador es tan sólo posible cuando estos han sido puestos a nuestra disposición. Si no se desea depositar sin más los datos en una caja fuerte, existen diferentes formas de acceder a ellos:

- alguien opera un ordenador y llama por teléfono al usuario de los datos,
- directamente desde la consola del ordenador (acceso físico),
- a través de un puerto serie, o
- a través de una red.

Todas estas alternativas deberían presentar un rasgo en común: cada uno se debería autenticar como usuario antes de poder acceder a los recursos o datos deseados. Dicho de otra forma: se debe haber demostrado una identidad que mediante una regla de acceso le permitirá acceder a los recursos (datos o acciones) requeridos. Un servidor de web puede ser en este aspecto algo diferente, pero en cualquier caso seguro que nadie desea que el servidor de web revele sus datos personales al primero que pase por allí.

El primer punto de la lista es el que más se asemeja al caso del ser humano. Por ejemplo, en el caso de un banco hay que demostrar al empleado que tiene derecho a acceder a su cuenta, ya sea mediante su firma, un PIN o una contraseña. De esta manera demostrará que usted es la persona que pretende ser. En algunos casos (que probablemente poco tienen que ver con ordenadores, sistemas operativos y redes) es posible ganarse la confianza del poseedor de una

información ofreciéndole con habilidad pequeños datos fragmentados sobre hechos de la naturaleza más diversa o mediante una hábil retórica de tal modo que poco a poco el individuo irá ofreciendo poco a poco más información sin darse cuenta. En los círculos hackers, a esto se le llama "Social Engineering". Contra este tipo de ataque sólo se puede actuar informando debidamente al personal y con un uso sensato de la información y del lenguaje. Los ataques a los sistemas informáticos a menudo van precedidos de un asedio de tipo Social-Engineering, contra el personal de recepción, el personal de servicio de la empresa o contra miembros de la familia. Este tipo de ataque no se suele detectar hasta mucho tiempo después.

Alguien que quiere acceder a ciertos datos de forma no autorizada puede utilizar el método más tradicional ya que el mismo hardware es un punto de ataque. El ordenador debe estar protegido contra robo, cambio, y sabotaje en sus piezas y en su unidad (así como el backup de sus datos). A este tipo de ataques pueden añadirse la conexión a una red o un cable eléctrico. El proceso de arranque debe de estar asegurado ya que una determinada combinación de teclas conocida puede producir en el ordenador una reacción concreta. Para evitar esto se pueden utilizar contraseñas para la BIOS y para el bootloader.

Si bien los puertos serie con terminales en serie son todavía habituales, apenas se siguen instalando en puestos de trabajo nuevos. En lo que respecta al tipo de ataque, una terminal en serie es un caso excepcional: no se trata de un puerto de red ya que para la comunicación entre las unidades del sistema no se utiliza ningún protocolo de red. Un simple cable (o un puerto infrarrojo) servirá de medio de transmisión para caracteres sencillos. El cable en sí es el punto de ataque más sencillo. Sólo hay que conectar una vieja impresora y recibir la información. Lo que es posible con una simple impresora se puede hacer también de otra forma a través de medios más sofisticados.

Dado que abrir un fichero en un ordenador está sometido a otras limitaciones de acceso que las de abrir una conexión en red a un servicio en un ordenador, hay que hacer distinción entre la seguridad local y la seguridad de red. La diferencia radica en que los datos deben ir ligados en paquetes para ser enviados y llegar a la aplicación.

Seguridad local

Como ya mencionamos, la seguridad local comienza con las características físicas del ordenador. Partimos de la suposición de que un ordenador está constituido de forma que la seguridad se adecua al nivel deseado y necesario. Colóquese en el papel de quien pretende "asaltar" un ordenador: mientras sigamos hablando de "seguridad local" la tarea consiste en diferenciar a unos usuarios de otros, de modo que ningún usuario pueda obtener los derechos de

otro usuario. Esta es la regla general, pero evidentemente un caso diferente es la cuenta `root`, que posee todos los derechos sobre el sistema. Cuando un usuario se convierte en `root`, puede transformarse en cualquiera de los usuarios locales sin necesidad de contraseña y de este modo leer cualquier fichero local.

Contraseñas

El sistema Linux no guarda en forma de texto legible las contraseñas que usted debería haber establecido, ya que en caso de que el fichero en el cual se guardan las contraseñas fuera robado, todas las cuentas de ese sistema estarían en peligro. En lugar de ello, el sistema codifica su contraseña y cada vez que usted introduzca su contraseña ésta será codificada y el resultado se comparará con la contraseña archivada. Esto naturalmente sólo tiene sentido si de la contraseña codificada no se puede deducir la contraseña en sí. El caso es como sigue: a este tipo de logaritmos se les denomina "logaritmos trampa" porque sólo funcionan en una dirección. Un atacante que haya obtenido una contraseña codificada no puede simplemente descodificarla y ver la contraseña. La única solución es probar una por una todas las combinaciones de letras posibles hasta dar con la contraseña que una vez codificada se parece a la que tenía. Se puede calcular rápidamente el gran número de contraseñas posibles que se pueden hacer combinando ocho letras.

En los años 70, un argumento a favor de este concepto de seguridad era que el algoritmo utilizado era muy lento y que necesitaba segundos para codificar una contraseña. Los PCs actuales pueden realizar desde varios cientos de miles hasta millones de codificaciones en un segundo lo que requiere dos cosas: las contraseñas codificadas no deben ser visibles para ninguno de los usuarios (`/etc/shadow` no puede ser leído por un usuario normal) y las contraseñas no deben ser fáciles de adivinar para el caso en que por un error se pudieran leer las contraseñas codificadas. Una contraseña como "fantasía" reescrita como "f@nt@s13" no resulta muy útil: Tales estrategias para despistar son un juego de niños para los programas de los piratas informáticos que utilizan diccionarios como fuente de consulta. Es mejor utilizar combinaciones de letras que no formen una palabra conocida y que sólo tengan sentido para uno mismo (pero que tampoco sea la combinación que abre el candado de la maleta). Una buena contraseña podrían ser las letras iniciales de las palabras de una frase. Por ejemplo: el título de un libro, "El nombre de la rosa" de Umberto Eco, encierra una buena contraseña: "EndlrUE". Una contraseña del tipo "Casanova" o "Lorena76" podría ser adivinada por alguien que le conozca más o menos bien.

El proceso de arranque

Evite que se pueda arrancar el sistema mediante un disquete o un CDROM, ya sea desmontando las unidades de lectura o seleccionando una contraseña BIOS

y determinando en la BIOS que el arranque se realice exclusivamente desde el disco duro.

Los sistemas Linux arrancan generalmente con un boot-loader, que permite transmitir opciones adicionales al kernel que se va a arrancar. Este tipo de acciones hacen peligrar la seguridad, en gran medida porque el kernel no sólo funciona con privilegios de usuario root sino porque es el que otorga desde un principio los privilegios root. Si utilizan LILO como boot-loader, puede evitar esto introduciendo otra contraseña adicional en `/etc/lilo.conf` (ver [El proceso de arranque y el gestor de arranque](#) en la página 73).

Permisos de acceso

Hay que partir del principio de que siempre se debe trabajar con el menor número de privilegios posible. En definitiva, no es necesario estar registrado como usuario root para leer o escribir e-mails. Si el programa de correo electrónico (MUA = Mail User Agent) con el que se trabaja tuviera un fallo, este repercutiría con los mismos derechos con los que se tenían activos en el momento del problema. Lo que se trata aquí es de minimizar los daños.

Los derechos individuales de los más de 200000 ficheros que se distribuyen con SuSE se otorgan de forma cuidadosa. El administrador de un sistema sólo debería instalar software adicional u otros ficheros con mucha precaución y siempre prestando atención especial a los derechos atribuidos a los ficheros. Un administrador experimentado y consciente de la importancia del tema de la seguridad siempre debe utilizar la opción `-l` en el comando `ls`, lo que le ofrecerá una lista completa de los ficheros incluyendo todos los derechos de acceso de tal forma que rápidamente podrá detectar si algún derecho no está bien adjudicado. Un atributo que no está bien adjudicado puede originar que un fichero pueda ser borrado o sobrescrito. Esto puede originar que los ficheros intercambiados puedan ser ejecutados también por root o que los ficheros de configuración de programas puedan ser utilizados como root. Alguien que atacara el sistema podría de este modo ampliar considerablemente sus derechos. A este tipo de intrusiones se les denomina "huevos de cuco" porque el programa (el huevo) es depositado en el nido por un usuario extraño (el pájaro) y ejecutado (incubado) de forma similar a cómo ocurre con el cuco que hace que otros pájaros incuben sus huevos.

Los sistemas SuSE disponen de ficheros `permissions`, `permissions.easy`, `permissions.secure` y `permissions.paranoid` en el directorio `/etc`. En estos ficheros se determinan derechos especiales sobre archivos como por ejemplo directorios de escritura universal o `setuser-ID-bits` (el programa no se ejecuta con la autorización del propietario del proceso que lo ha arrancado sino con la autorización del propietario del fichero, que por norma general es root). El

fichero `/etc/permissions.local` está a disposición del administrador; aquí podrá guardar sus propias modificaciones. Para definir con comodidad cuáles son los ficheros usados por los programas de configuración de SuSE para la adjudicación de los permisos existe el punto del menú ‘Seguridad’ de YaST. En el fichero `/etc/permissions` y en la página de manual del comando `chmod` (`man chmod`) se recoge más información sobre este tema.

Buffer overflows, format string bugs

Siempre que un programa procesa datos que de una forma u otra están o han estado bajo la influencia de un usuario se requiere mucha precaución. Principalmente esto afecta a los programadores de la aplicación: Un programador debe garantizar que los datos serán bien interpretados por el programa, que en ningún momento se escribirán en sectores de memoria demasiado pequeños y se responsabilizará de que su propio programa entregue los datos adecuadamente y a través de las interfaces predefinidas para ello.

Hablamos de que se ha producido un “buffer overflow” cuando al definir un sector de la memoria del búfer no se tiene en cuenta el tamaño del búfer. Puede ocurrir que los datos (que provienen de un usuario) ocupen más espacio del que hay disponible en el búfer. Al reescribir el búfer más allá de sus límites puede ocurrir que (en vez de sólo procesar los datos) el programa ejecute secuencias de programas estando éstas bajo el control del usuario y no así del programador. Este es un error grave, especialmente cuando el programa corre con derechos especiales (véase derechos de acceso más arriba). Los llamados “format string bugs” funcionan de un modo algo distinto, pero utilizan igualmente user-input para desviar el programa de su camino real.

Estos errores de programación son aprovechados (ingl. *exploit*) por programas que se ejecutan con privilegios superiores, o sea programas del tipo `setuid` y `setgid`. Es posible protegerse y proteger el sistema frente a este tipo de errores retirando del programa los derechos privilegiados de ejecución. Aquí también es válido el principio de otorgar privilegios lo más bajos posible (véase el apartado sobre los derechos de acceso).

Dado que los “buffer overflows” y los “format string bugs” son errores en el tratamiento de los datos del usuario, no son necesariamente “explotados” sólo cuando se dispone de acceso a un “login” local. Muchos de estos errores, ya conocidos, pueden ser “explotados” a través de una conexión en red. Por esta razón, no es posible determinar si los “buffer overflows” y los “format string bugs” han sido originados por el ordenador local o por la red.

Virus

En contra de lo que se cree, sí existen virus para Linux. Los virus conocidos fueron denominados “Proof-of-Concept” por sus autores para demostrar que

esta técnica funciona. Sin embargo no se ha observado ninguno de estos virus en "libertad".

Para desarrollarse y sobrevivir, los virus necesitan un huésped. Este huésped es un programa o un sector de memoria de importancia para el sistema, como p.ej. el Master-Boot-Record, y el código de programa del virus debe tener acceso de escritura a éste. Debido a sus características multi-usuario, Linux puede limitar el derecho de escritura de los archivos, especialmente de los ficheros de sistema. Es decir, que si se trabaja como `root`, aumentan las posibilidades de que su sistema sea infectado por un virus de este tipo. Por lo tanto, tenga en cuenta el principio del menor privilegio posible. De este modo, lo difícil sería que su sistema se pudiera llegar a infectar con un virus trabajando bajo Linux. Por otra parte, no debería ejecutar un programa que haya bajado de Internet y cuyo origen desconoce. Los paquetes SuSE-rpm están firmados de forma criptográfica. Estas firmas digitales avalan el esmero de SuSE al elaborar el paquete. Los virus son un clásico síntoma de que un sistema altamente seguro se vuelve inseguro cuando el administrador o el usuario no asumen con seriedad el tema de la seguridad.

No hay que confundir los virus con los gusanos, que también son fenómenos relacionados con las redes pero que no necesitan un huésped para propagarse.

La seguridad en la red

La misión de la seguridad local es diferenciar entre los usuarios de un ordenador, en particular el usuario `root`. Por el contrario, la seguridad de la red consiste en proteger el sistema entero contra ataques provenientes de la red. Si bien al registrarse en el sistema de la manera convencional se deben introducir un nombre de usuario y una contraseña, la identificación del usuario es más un tema de seguridad local. Al registrarse en la red hay que considerar dos aspectos de seguridad: lo que sucede hasta que se ha conseguido con éxito la autenticación (seguridad de red) y lo que ocurre posteriormente (local).

X windows (Autenticación X11)

Como ya se ha mencionado anteriormente, la "transparencia respecto a la red" es una de las características básicas del sistema Unix. Esto es así sin lugar a dudas en el caso de X11, el sistema windowing de los sistemas Unix. Permite registrarse sin más en un ordenador remoto e iniciar un programa que se podrá ver en el propio ordenador a través de la red.

Cuando nuestro servidor X tiene que mostrar un cliente X a través de la red, debe proteger los recursos que gestiona (el display) contra accesos no autorizados. En este caso concreto, esto significa que el programa cliente tiene que

recibir derechos. En X-Windows esto sucede de dos formas: Controles de acceso basados en host y controles basados en cookies. Los primeros están basados en la dirección IP del ordenador en el que se debe ejecutar el programa cliente y se controlan con el programa `xhost`. El programa `xhost` introduce la dirección IP de un cliente legítimo en una mini base de datos en el servidor X. Pero limitarse a establecer una única autentificación en una dirección IP no es precisamente seguro. Otro usuario podría estar activo en el ordenador con el programa cliente y tendría acceso al servidor X como si hubiera robado la dirección IP. Por esta razón aquí no profundizaremos más sobre estos métodos. La manpage del comando `xhost` ofrece más explicaciones sobre el funcionamiento (y también contiene la advertencia).

Los controles de acceso basados en "cookies" utilizan como medio de identificación una cadena de caracteres que sólo conocen el servidor X y el usuario registrado legítimamente. El cookie se utiliza como método de identificación similar a una contraseña. Al hacer login, este "cookie" (la palabra inglesa *cookie* significa galleta y aquí hace referencia a las galletas chinas de la fortuna, que contienen un refrán en su interior) se graba en el fichero `.Xauthority` del directorio personal del usuario y de este modo, está a disposición de cualquier cliente de X Windows que quiera abrir una ventana en X-server. El programa `xauth` ofrece al usuario la herramienta para explorar el fichero `.Xauthority`. No se podrán abrir más ventanas de nuevos clientes X si `.Xauthority` se borra del directorio personal o si se le cambia el nombre. Para ampliar información sobre el tema de la seguridad de Windows X le recomendamos la manpage de `Xsecurity` (`man Xsecurity`).

`ssh` (secure shell) puede transmitir la conexión a un servidor X de forma transparente (o sea, no directamente visible) para un usuario a través de una conexión de red completamente codificada. En tal caso se habla de "X11-forwarding". En este caso, en el lado del servidor se simula un servidor X y en la shell del lado remoto se coloca la variable `DISPLAY`.

Aviso

Si considera que el ordenador en el que se está registrando no es lo suficientemente seguro, no debería dejar que se realicen conexiones X-windows. Con el "X11-forwarding" conectado, los piratas podrían autenticarse y conectarse con su servidor X a través de su conexión `ssh` y, p. ej., espiar su teclado.

Aviso

Buffer overflows y format string bugs

Lo dicho sobre "buffer overflows" y "format string bugs" en el apartado de "seguridad local", se aplica también a la seguridad de red, si bien aquí estos errores

ya no pueden ser directamente clasificados como locales o remotos. Del mismo modo que en las variantes locales de estos errores de programación, por lo general en los servicios de red los búfer Overflows tienen como objetivo los privilegios de `root`. De no conseguir directamente acceso a los privilegios `root`, el pirata podría abrirse camino hasta una cuenta local con pocos privilegios en la cual podría aprovecharse de problemas de seguridad (locales), en caso de que existieran.

Las variantes más comunes de ataque remoto a través de la red son los búfer overflows y los format string bugs. Mediante listas de correo de seguridad se distribuyen los llamados "exploits", que no son más que programas que aprovechan los puntos débiles hallados recientemente. Así mismo las personas que no conozcan con lujo de detalles estos puntos débiles o lagunas pueden aprovecharse de ellas. Con el paso de los años se ha demostrado que el hecho de que estos "exploitcodes" circulen libremente ha contribuido a que la seguridad de los sistemas operativos aumente debido a que los productores de sistemas operativos se ven obligados a solucionar los problemas de su software. En el caso del software cuyo source-code se distribuye de forma libre (SuSE Linux es distribuido con todas las fuentes disponibles), alguien que encuentre una laguna con "exploitcodes" puede ofrecer al mismo tiempo una sugerencia para solventar el problema.

DoS - Denial of Service

El objetivo de este tipo de ataques es el de interrumpir el servicio (o incluso todo el sistema). Esto puede llevarse a cabo de las maneras más diversas: Por sobrecarga, ocupando el sistema con paquetes absurdos o mediante el uso de "remote buffer overflows", que no pueden ser utilizados de forma directa para ejecutar programas en la unidad remota.

En la mayoría de los casos, un DoS encuentra su justificación en el hecho de que un servicio simplemente ya no esté disponible. El hecho de que un servicio falte puede traer consigo una serie de consecuencias. Véase "man in the middle: sniffing, tcp connection hijacking, spoofing" y "DNS poisoning".

man in the middle: sniffing, tcp connection hijacking, spoofing

De forma general se denomina con el término "man in the middle attack" al ataque que se realiza desde la red y en el cual el atacante ocupa una posición intermedia entre dos unidades que se comunican. Todos tienen por lo general una cosa en común: la víctima no se percató de nada. Existen muchas variaciones: el atacante intercepta la comunicación y para que la víctima no se percate de nada, establece él mismo una comunicación con la máquina objetivo. Sin darse cuenta, la víctima ha abierto una comunicación con el ordenador equivocado que

se hace pasar por su objetivo. La forma más sencilla de "man in the middle attack" es el "sniffer". Simplemente espía las conexiones de red que pasan por él (sniffing = ingl. fisgonear). Todo se vuelve más complicado cuando el atacante de por medio intenta tomar posesión de una conexión ya establecida (hijacking = ingl. secuestrar). Para ello, el atacante tiene que ir analizando durante algún tiempo los paquetes que van pasando de largo para poder prever la secuencia de números TCP correcta de la conexión TCP. Cuando consigue asumir el papel del objetivo de la conexión, la víctima lo nota ya que de su lado la conexión finaliza como no válida. El atacante se aprovecha sobre todo de protocolos que no estén protegidos de forma criptográfica contra "hijacking" y en los cuales al inicio de la conexión se realiza una autenticación. Se denomina "spoofing" al envío de paquetes con datos de remitente modificados; por lo general la dirección IP. La mayoría de los ataques requieren el envío de paquetes falsificados, lo cual en Unix/Linux sólo puede ser realizado por el superusuario (root).

Muchas de las modalidades de ataque vienen acompañadas de un DoS. Si se ofrece la oportunidad de separar un ordenador de la red de forma súbita (aunque sea sólo un momento) se facilita el poder realizar un ataque activo ya que tras ello no se esperarían más problemas.

DNS poisoning

El pirata intenta "envenenar" ((ingl. *poisoning*)) el cache de un servidor DNS por medio de un paquete respuesta DNS falsificado ("spoofed") para que entregue la información deseada a una víctima que la solicita. Generalmente el atacante deberá recibir algunos paquetes del servidor y analizarlos para poder introducir de forma verosímil esta información a un servidor DNS. Dado que muchos servidores han configurado una relación de confianza con los demás ordenadores mediante sus direcciones IP o los hostnames, puede que uno de estos ataques pueda dar frutos rápidamente a pesar del trabajo que conlleva. No obstante, una condición para conseguirlo es un buen conocimiento de la estructura de confianza existente entre estos ordenadores. En la mayoría de los casos el atacante no puede evitar que se tenga que ejecutar un DoS perfectamente sincronizado contra un servidor DNS cuyos datos se desean falsificar.

Esto se puede remediar mediante el uso de una conexión codificada de forma criptográfica, la cual puede verificar la identidad del objetivo de la conexión.

Gusanos

A menudo se equipara a los gusanos con los virus, pero existe una gran diferencia entre ellos: un gusano no tiene que infectar un programa huésped y su especialidad consiste en expandirse lo más rápidamente posible por la red. Algunos gusanos conocidos, como son p.ej. Ramen, Lion y Adore, hacen uso de

lagunas muy populares en programas de servidor como `bind8` o `lprNG`. Es relativamente fácil protegerse contra los gusanos, ya que desde el momento en el que se detecta la laguna y hasta que aparece el gusano suelen transcurrir varios días, permitiendo que aparezcan paquetes de update. Naturalmente es requisito indispensable que el administrador del sistema instale los Security-updates en su sistema.

Trucos y consejos: indicaciones generales

Información: Para asegurar una gestión eficiente de la seguridad es necesario estar al día sobre los últimos desarrollos y los problemas de seguridad más recientes. Una muy buena protección contra todo tipo de fallos consiste en implementar de la forma más rápida posible los paquetes de update que se anuncien en un Security-Announcement. Los anuncios de seguridad de SuSE se distribuyen a través de una lista de correo en la que usted puede inscribirse siguiendo los enlaces que encontrará en <http://www.suse.de/security.suse-security-announce@suse.de> es la primera fuente de información sobre paquetes de actualización donde el equipo de seguridad publica la información más actual.

La lista de correo suse-security@suse.de es un foro de discusión en el que se puede obtener mucha información sobre el tema de la seguridad. Para apuntarse en la lista hay que dirigirse a la misma URL utilizada para obtener información sobre actualizaciones: suse-security-announce@suse.de.

Una de las listas de correo sobre seguridad más conocidas del mundo es la lista bugtraq@securityfocus.com. Le recomendamos encarecidamente leer esta lista en la que aparece una media de 15 a 20 mensajes al día. En <http://www.securityfocus.com> encontrará más información.

A continuación se recogen algunas normas fundamentales que puede ser recomendable tenerlas en cuenta:

- Evite trabajar como `root`, siguiendo el principio de utilizar el mínimo privilegio posible para una tarea. Esto reduce las posibilidades de un hueco de cuco o un virus y de este modo evitará problemas.
- Use conexiones codificadas siempre que le sea posible para ejecutar tareas remotas. "ssh" (secure shell) es estándar. Evite `telnet`, `ftp`, `rsh` y `rlogin`.
- No utilice métodos de autenticación que estén únicamente basados en la dirección IP.

- Mantenga siempre actualizados sus paquetes más importantes para trabajar en la red y abónese a las listas de correo de anuncios acerca del software correspondiente (p.ej.: `bind`, `sendmail`, `ssh`). Esto también es válido para la seguridad local.
- Optimice los derechos de acceso de los ficheros del sistema que sean de importancia para la seguridad adaptando el fichero `/etc/permissions` de su elección a sus necesidades. Un programa `setuid` que ya no tenga un `setuid-bit` tal vez ya no pueda desempeñar realmente su función pero por norma general ya no constituye un problema de seguridad. Es recomendable proceder de forma similar con los ficheros y los directorios con acceso de escritura universal.
- Desactive todos los servicios de red que no sean estrictamente necesarios para su servidor. Esto hace que su servidor sea más seguro y evita que sus usuarios se acostumbren a usar un servicio que usted nunca ha puesto voluntariamente a su disposición (*legacy-Problem*). Con el programa `netstat` encontrará los puertos abiertos (con el estado de sockets `LISTEN`). Se puede utilizar con las opciones `netstat -ap` o `netstat -anp`. Con la opción `-p` se puede ver directamente qué proceso ocupa un puerto y con qué nombre.

Compare los resultados que ha obtenido con los de un `portscan` completo de su ordenador desde fuera. El programa `nmap` es ideal para ello. Revisa cada uno de los puertos y según la respuesta de su ordenador puede extraer conclusiones sobre un servicio que se encuentra en espera detrás del puerto. Nunca escanee un ordenador sin la aprobación directa del administrador ya que esto podría ser interpretado como un acto de agresión. No es suficiente con escanear los puertos TCP. También deberá escanear los puertos UDP (opciones `-ss` y `-su`).

- Para realizar una prueba de integridad de confianza de los archivos que se encuentran en su sistema deberá utilizar `tripwire` y codificar la base de datos para protegerla de manipulaciones. Además necesitará hacer un backup de esta base de datos en un dispositivo de almacenamiento de datos que se encuentre fuera de la máquina y que no esté conectado con la red a través del ordenador.
- Tenga cuidado a la hora de instalar software extraño. Ya se ha dado el caso de que un pirata haya incluido un caballo de Troya en los archivos `tar` de un software de seguridad. Por suerte esto se detectó a tiempo. Si instala un paquete binario, debería estar seguro de su procedencia.

Los paquetes `rpm` de SuSE se distribuyen con la firma `gpg`. La clave que utilizamos para firmarlos 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 paket.rpm` muestra si la suma de control y la firma del paquete (¡no instalado!) se corresponden. La clave se encuentra en el primer CD de distribución SuSE a partir de SuSE-7.1 y en la mayoría de los servidores de códigos (keyserver) del mundo.

- Compruebe regularmente el backup de los datos y de su sistema. En determinadas circunstancias, si la información de la función del backup no es precisa, el backup carece de utilidad.
- Revise sus "Logfiles". En la medida de lo posible debería escribir un pequeño script que se encargue de buscar entradas irregulares en sus logfiles. Esta tarea no es para nada trivial ya que sólo usted sabe qué es irregular y qué no lo es.
- Utilice `tcp_wrapper` para restringir el acceso a los diferentes servicios de su ordenador mediante un IP. Sólo aquellas direcciones IP que tengan permiso explícito podrán acceder a unos determinados servicios. En las páginas de manual `tcpd(8)` y `hosts_access` (`man tcpd`, `man hosts_access`) encontrará más información sobre `tcp_wrapper`.
- Puede utilizar el firewall (cortafuegos) SuSE como protección adicional a `tcpd` (`tcp_wrapper`).
- Ponga en práctica sus conceptos de seguridad de forma redundante: un mensaje que llega dos veces es mejor que uno que no llega nunca. Esto también es válido para las conversaciones con los compañeros.

Informe a SuSE sobre nuevos problemas de seguridad

Si encuentra un problema de seguridad (por favor compruebe los paquetes de actualización existentes) remítase entonces con toda confianza a la dirección de e-mail security@suse.de. Le rogamos que adjunte una descripción detallada del problema así como el número de versión del paquete utilizado. Procuraremos contestarle a la mayor brevedad posible. Es preferible que envíe su e-mail con una codificación gpg. Nuestra clave gpg 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 se puede bajar desde <http://www.suse.de/security>.

Parte V

Anexo

Sistemas de archivos en Linux

Linux soporta una gran variedad de sistemas de archivos. Este capítulo ofrece una breve introducción a los sistemas de archivos más conocidos en Linux, prestando una especial atención a su estructura y ventajas así como a sus campos de aplicación. Asimismo se presentará información sobre el soporte de archivos grandes o "Large File Support".

Glosario

Metadatos Garantiza la estructura interna de datos, el orden de la estructura y la disponibilidad de los datos en el disco duro. En resumidas cuentas, se trata de los "datos sobre los datos". Todo sistema de archivos posee su propia estructura de metadatos. Aquí es donde se encuentra en parte la razón de las diferencias en cuanto a rendimiento de los sistemas de archivos. Es extremadamente importante mantener intactos los metadatos, ya que de lo contrario todo el sistema de archivos se vería perturbado.

Inode Los inodes contienen toda la información respecto a un archivo: el nombre, el tamaño, el número de enlaces, la fecha, la hora en que fue creado, modificaciones, accesos como "señalador" (ingl. *pointer*) de los bloques del disco duro y dónde se encuentra grabado.

Journal En relación a un sistema de archivos, un journal o diario es una estructura interna del disco con un tipo de protocolo en el que el controlador del sistema de archivos introduce los (meta)datos del sistema de archivos que van a ser modificados. El "journaling" reduce enormemente el tiempo de elaboración de un sistema Linux, ya que de este modo el controlador del sistema de archivos no debe iniciar una búsqueda de los metadatos modificados en todo el disco. En vez de eso, basta con ver las entradas del diario.

Los sistemas de archivos más importantes en Linux

Contrariamente a lo que ocurría hace dos o tres años, la elección de un sistema de archivos en Linux ya no es una cuestión de segundos ("¿Ext2 o ReiserFS?"). A partir de la versión 2.4, el kernel ofrece una gran selección de sistemas de archivos. A continuación le mostramos un resumen de las funciones básicas de estos sistemas de archivos y sus ventajas.

Tenga siempre en cuenta que no existe ningún sistema de archivos que puede funcionar del mismo modo con todas las aplicaciones. Cada sistema de archivos tiene puntos fuertes y débiles que se deben de tener presentes. Ni el sistema de archivos más desarrollado de todo el mundo puede sustituir a la copia de seguridad.

Los conceptos "integridad de los datos" o "consistencia de los datos" no se refieren en este capítulo a la consistencia de los datos guardados de un usuario (los datos que las aplicaciones que utiliza escribe en sus archivos). La consistencia de estos datos debe quedar asegurada por las aplicaciones mismas.

Atención

Configuración de sistemas de archivos

Mientras no se indique lo contrario explícitamente, todas las acciones de particionamiento así como de creación y edición de sistemas de archivos pueden llevarse a cabo cómodamente con YaST.

Atención

Ext2

El origen de Ext2 se remonta a los primeros días de Linux. Su antecesor, el Extended File System fue implementado en abril de 1992 e integrado en Linux 0.96c. Este sufrió una serie de modificaciones y durante años se le conoció como Ext2 a la vez que se le consideró el sistema de archivos más popular de Linux. Con la introducción del sistema Journaling File y de su tiempo de elaboración tan sorprendentemente corto, Ext2 perdió importancia.

Puede que le sirva de ayuda un pequeño resumen de los puntos fuertes de Ext2 para que comprenda su popularidad entre los usuarios de Linux, que en cierta medida aún hoy lo prefieren como sistema de archivos.

Estabilidad Con el correr del tiempo, Ext2 ha sufrido muchas mejoras que le han dado el sobrenombre de “roca sólida” (ingl. *rock-solid*). En caso de una caída del sistema en la que el sistema de archivos no puede desmontarse adecuadamente, `e2fsck` inicia un análisis de los datos del sistema de archivos. Los metadatos se reconstruyen y los archivos o bloques de datos que quedan sueltos se guardan en un directorio denominado `lost+found`. En contraposición a (la mayoría) de los sistemas de archivos transaccionales o journaling, `e2fsck` analiza todo el sistema de archivos y no sólo los bits de metadatos modificados. Esto dura más tiempo que la comprobación de los datos de protocolo de un sistema journaling. Dependiendo del tamaño del sistema de archivos, puede llegar a durar más de media hora. Por esta razón, Ext2 no se escoge para ningún servidor que deba tener un alto rendimiento. Debido a que Ext2 no debe hacerse cargo de ningún diario y a la vez necesita poca memoria, a menudo es más rápido que otros sistemas de archivos.

Fácil actualización Tomando como base la fortaleza de Ext2, Ext3 podría llegar a convertirse en el sistema de archivos de la próxima generación. Su fiabilidad y estabilidad se encontrarían a la par de las ventajas de un sistema de archivos journaling.

Ext3

Ext3 fue concebido por Stephen Tweedie. A diferencia del resto de los sistemas de archivos de “última generación”, no está basado en un nuevo diseño, sino en Ext2. Ambos sistemas de archivos están estrechamente vinculados. Un sistema de archivos Ext3 se puede montar fácilmente sobre un sistema Ext2. La diferencia fundamental entre ambos radica en que Ext3 también soporta journaling.

Estas son brevemente las tres ventajas de Ext3:

Actualización fácil y muy fiable de Ext2 Ya que Ext3 se basa en el código de Ext2, a la vez que comparten formato tanto para el disco como para los metadatos, las actualizaciones no son complicadas. Incluso se pueden llevar a cabo mientras el sistema de archivos Ext2 está montado. El proceso de cambio a otro sistema de archivos journaling, como p. ej. ReiserFS, JFS, o XFS, puede llegar a ser muy trabajoso debido a que se deben realizar copias de seguridad de todo el sistema de archivos y después instalarlo desde cero. Sin embargo, el cambio a Ext3 puede ser una cuestión de minutos. Además es muy seguro, ya que resulta difícil que la reelaboración de todo un sistema de archivos desde cero no tenga errores. Si se tiene en

cuenta la cantidad de sistemas Ext2 disponibles que esperan una actualización a un sistema de archivos journaling, se puede imaginar fácilmente el significado de Ext3 para muchos administradores de sistemas. El pasar de Ext3 a Ext2 es tan fácil como la actualización en sentido contrario. Tan sólo tiene que desmontar el sistema Ext3 y montarlo como Ext2.

Fiabilidad y rendimiento Todos los sistemas de archivos journaling siguen el principio de "sólo metadatos" (ingl. *metadata-only*). Esto significa que los metadatos permanecen en un estado consistente, lo que sin embargo no puede ser garantizado automáticamente para los datos del sistema de archivos. Ext3 tiene capacidad para cuidar tanto de los metadatos como de los datos mismos. Se puede configurar individualmente el detalle con el que Ext3 debe ocuparse de los datos y metadatos. El grado más alto de seguridad (esto es, integridad de los datos) se consigue al arrancar Ext3 en modo `data=journal`; esto puede hacer que el sistema sea más lento, ya que se guardarán en el diario tanto los datos como los metadatos. Una posibilidad relativamente nueva consiste en la utilización del modo `data=ordered`, que garantiza la integridad tanto de los datos como de los metadatos, a pesar de que sólo realiza journaling para los metadatos. El controlador del sistema de archivos reúne todos los bloques de datos relacionados con la actualización de los metadatos. Estos bloques quedan agrupados como "transacción" en los discos, antes de que los metadatos sean actualizados. Con esto se consigue consistencia de datos y metadatos sin pérdida de rendimiento. Un tercer tipo de modo es `data=writeback`. De esta forma se puede escribir datos en el sistema de archivos principal, después de que los metadatos hayan pasado al diario. Para muchos esta opción es la mejor configuración en cuanto a rendimiento. Sin embargo, con esta opción puede ocurrir que aparezcan viejos datos en los archivos después de haberse producido una caída del sistema, a la vez que se garantiza la integridad del sistema de archivos. Mientras no se indique otra opción, Ext3 arrancará con la opción por defecto `data=ordered`.

Truco**Conversión de un sistema de archivos Ext2 a Ext3**

La conversión de un sistema de archivos Ext2 a un sistema de archivos Ext3 se lleva a cabo en dos pasos:

Crear el diario (journal): Ejecute el comando `tune2fs -j` como usuario `root`. `tune2fs` se encarga de crear el diario Ext3 con parámetros estándar. Si por el contrario prefiere definir usted mismo con qué tamaño y en qué dispositivo debe crearse el diario, ejecute `tune2fs -J` con ambos parámetros `size=` y `device=`. Puede obtener información adicional sobre `tune2fs` en las páginas del manual (`man 8 tune2fs`).

Determinar el tipo de sistema de archivos en `/etc/fstab` Para que el sistema de archivos Ext3 sea detectado como tal, abra el archivo `/etc/fstab` y cambie el tipo de sistema de archivos de la partición correspondiente de `ext2` a `ext3`. La modificación se aplicará tras reiniciar el sistema.

Truco**ReiserFS**

Oficialmente una de las funciones principales de la versión 2.4 del kernel, ReiserFS está disponible desde la versión 6.4 de SuSE Linux como parche para el kernel de SuSE 2.2.x. ReiserFS es producto de Hans Reiser y del equipo de desarrollo Namesys. ReiserFS se ha perfilado como una alternativa poderosa a Ext2. Sus grandes ventajas son: una mejor administración de la memoria del disco duro, un mejor rendimiento del acceso al disco y una recuperación más rápida después de una caída del sistema. No obstante, ReiserFS concede mucha importancia a los metadatos pero no a los datos en sí. La próxima generación de ReiserFS incluirá data-journaling (se escribirán tanto datos como metadatos en el diario) así como accesos de escritura (véase `data=ordered` en Ext3).

Los principales ventajas de ReiserFS en detalle:

Mejor administración de la memoria del disco duro En ReiserFS, todos los datos se organizan en una estructura llamada B*-balanced tree. La estructura de árbol contribuye a una mejor administración de la memoria del disco duro, ya que los archivos pequeños se pueden guardar directamente en las hojas de B*trees, en vez de guardarlos en otro lugar y luego tener

que administrar el señalador (ingl. *pointer*) para que apunte al sitio indicado. Además, la memoria no se asignará en unidades de 1 a 4 Kb, sino en la unidad necesaria. Otra ventaja es el proceso dinámico de inodes. Esto dota al sistema de archivos de una gran flexibilidad frente a los sistemas convencionales, como por ejemplo Ext2, en el que se debe indicar la anchura del inode en el momento de crear el sistema de archivos.

Mejor rendimiento del acceso al disco duro Se habrá dado cuenta de que en los archivos pequeños, tanto los datos del archivo como la información (inode) de "stat_data" se guardan uno al lado del otro. Basta con un único acceso al disco duro para suministrar toda la información necesaria.

Rápida recuperación tras una caída del sistema Desde el contenido de un diario al seguimiento de las pequeñas modificaciones de metadatos, la comprobación del sistema de archivos se reduce a unos pocos segundos incluso en sistemas de archivos grandes.

JFS

JFS, "Journaling File System", fue desarrollado por IBM para AIX. La primera versión beta de JFS portada a Linux llegó al entorno Linux en el verano del año 2000. La versión 1.0.0 salió a la luz en el año 2001. JFS está diseñado para cumplir las exigencias del entorno de un servidor de alto rendimiento. Al ser un sistema de archivos de 64 bits, JFS soporta archivos grandes y particiones LFS (ingl. *Large File Support*), lo cual es una ventaja más para los entornos de servidor.

Un vistazo más detallado a JFS muestra por qué este sistema de archivos es una buena elección para su servidor Linux:

Journaling eficaz JFS, al igual que ReiserFS, sigue el principio de "metadata only". En vez de una comprobación completa, sólo se tienen en cuenta las modificaciones en los metadatos provocadas por las actividades del sistema. Esto ahorra una gran cantidad de tiempo en la fase de recuperación del sistema tras una caída. Las actividades simultáneas que requieren más entradas de protocolo se pueden unir en un grupo, en el que la pérdida de rendimiento del sistema de archivos se reduce en gran medida mediante múltiples procesos de escritura.

Eficiente administración de directorios JFS abarca diversas estructuras de directorios. En pequeños directorios se permite el almacenamiento directo del contenido del directorio en su inode. En directorios más grandes se

utilizan B⁺ trees, que facilitan considerablemente la administración del directorio.

Mejor utilización de la memoria mediante la adjudicación dinámica de inodes

En Ext2 es necesario indicar el grosor del inode (la memoria ocupada por la información de administración) por adelantado. Con ello se limita la cantidad máxima de archivos o directorios de su sistema de archivos.

Esto no es necesario en JFS, puesto que asigna la memoria inode de forma dinámica y la pone a disposición del sistema cuando no se está utilizando.

XFS

Pensado originariamente como sistema de archivos para sistemas operativos IRIX, SGI comenzó el desarrollo de XFS ya a principios de la década de los noventa. Con XFS consigue un sistema de archivos journaling de 64 bits de gran rendimiento adaptado a las necesidades extremas de la actualidad. XFS también está indicado para el trabajo con archivos grandes y ofrece un buen rendimiento en hardware de última generación. Sin embargo XFS, al igual que ReiserFS, tiene la desventaja de conceder mucha importancia a la integridad de los metadatos y muy poca a la de los datos:

Un breve resumen de las funciones clave de XFS aclarará por qué puede llegar a convertirse en un fuerte competidor de otros sistemas de archivos journaling en el tratamiento de datos.

Manejo de "grupos de asignación" (ingl. *allocation groups*) En el momento de la creación de un sistema de archivos XFS, el dispositivo de bloque (ingl. *block-device*) que sirve de base al sistema de archivos se divide en ocho o más campos lineales de igual tamaño denominados grupos de asignación. Cada grupo de asignación administra inodes así como memoria libre. Se puede considerar a estos grupos prácticamente como sistemas de archivos dentro de sistemas de archivos. Puesto que estos grupos de asignación son bastante independientes, el kernel puede dirigirse a más de uno simultáneamente. Este concepto de grupos de asignación independientes satisface los requisitos de los sistemas con varios procesadores.

Alto rendimiento con eficiente administración de la memoria del disco B⁺ trees administran la memoria libre y los inodes dentro de los grupos de asignación. El manejo de B⁺ trees contribuye al gran rendimiento de XFS. Una función única y característica de XFS es la llamada asignación retardada. XFS realiza la asignación de la memoria mediante la división en dos de los procesos. Una transacción "en suspenso" queda guardada en

RAM y el espacio en la memoria queda reservado. XFS aún no decide dónde exactamente (en qué bloque del sistema de archivos) se almacenan los datos. Esta decisión se retrasará hasta el último momento. Con esto, algunos datos temporales no quedan nunca almacenados en el disco, ya que cuando llegue el momento de decidir el lugar de almacenamiento ya estarán obsoletos. Así, XFS aumenta el rendimiento y disminuye la fragmentación del sistema de archivos. Debido a que una asignación retardada tiene como consecuencia menos procesos de escritura que en otros sistemas de archivos, es probable que la pérdida de datos tras una caída del sistema durante el proceso de escritura sea mayor.

Preasignación para evitar la fragmentación del sistema de archivos Antes de la escritura de los datos en el sistema de archivos, XFS reserva el espacio de memoria necesario para un archivo que vaya a ser asignado. De esta forma se reduce enormemente la fragmentación del sistema de archivos y el rendimiento aumenta, ya que el contenido de los archivos no queda dividido por todo el sistema de archivos.

Otros sistemas de archivos soportados

En la tabla A.1 en la página siguiente se incluyen otros sistemas de archivos soportados por Linux. Principalmente se soportan para garantizar la compatibilidad y el intercambio de datos entre distintos medios o sistemas operativos.

cramfs	<i>Compressed ROM file system</i> : un sistema de archivos comprimido con permiso de lectura para ROMs.
hpfs	<i>High Performance File System</i> : el sistema de archivos estándar de IBM OS/2 — sólo se soporta en modo de lectura.
iso9660	sistema de archivos estándar en CD-ROMs.
minix	este sistema de archivos tuvo su origen en proyectos académicos sobre sistemas operativos y fue el primero en ser utilizado en Linux. Hoy en día se utiliza como sistema de archivos para disquetes..
msdos	<i>fat</i> , utilizado originariamente en DOS, hoy en día es utilizado por distintos sistemas operativos.
ncpfs	para montar volúmenes Novell a través de una red.

Cuadro A.1: Continúa en la página siguiente...

<code>nfs</code>	<i>Network File System</i> : posibilita el almacenamiento de datos en el ordenador que se elija dentro de una red y permite garantizar el acceso a través de la red.
<code>smbfs</code>	<i>Server Message Block</i> : utilizado por productos como por ejemplo Windows para el acceso de archivos a través de una red.
<code>sysv</code>	utilizado en SCO UNIX, Xenix y Coherent (sistemas UNIX comerciales para PCs).
<code>ufs</code>	utilizado en BSD, SunOS y NeXTstep. Sólo se soporta en modo de lectura.
<code>umsdos</code>	<i>UNIX on MSDOS</i> : sistema de archivos a base de <code>fat</code> , que emula las características de Unix (derechos, enlaces, nombres de archivo largos) mediante archivos especiales.
<code>vfat</code>	<i>Virtual FAT</i> : Extensión del sistema de archivos <code>fat</code> (soporta nombres de archivo largos).
<code>ntfs</code>	<i>Windows NT file system</i> , sólo permiso de lectura.

Cuadro A.1: Sistemas de archivos en Linux

Soporte de archivos grandes en Linux

Al principio Linux sólo soportaba archivos con un tamaño máximo de 2 Gb. Debido a la creciente utilización de Linux por ejemplo en la administración de bases de datos o en la edición de datos de audio y vídeo, se ha hecho necesario el modificar el kernel y la librería GNU C (*glibc*) para que soporten archivos mayores de 2 Gb y se han introducido nuevas interfaces que pueden ser utilizadas por las aplicaciones. Hoy en día (casi) todos los sistemas de archivos importantes soportan LFS (Large File System – sistema de archivos grandes), lo que permite la edición de datos de gama alta.

La tabla A.2 en la página siguiente ofrece un resumen de las limitaciones actuales de los archivos de Linux y los sistemas de archivos para el kernel 2.4.x.

Sist. de archivos	Tamaño máx. archivo [Byte]	Tamaño máx.sist.arch.[Byte]
Ext2 oder Ext3 (1 kB tamaño bloque)	2^{34} (16 GB)	2^{41} (2 TB)
Ext2 oder Ext3 (2 kB tamaño bloque)	2^{38} (256 GB)	2^{43} (8 TB)

Ext2 oder Ext3 (4 kB tamaño bloque)	2^{41} (2 TB)	2^{44} (16 TB)
Ext2 oder Ext3 (8 kB tamaño bloque) (sistema con pages de 8 kB (como Alpha))	2^{46} (64 TB)	2^{45} (32 TB)
ReiserFS 3.5	2^{32} (4 GB)	2^{44} (16 TB)
ReiserFS 3.6 (en Linux 2.4)	2^{60} (1 EB)	2^{44} (16 TB)
XFS	2^{63} (8 EB)	2^{63} (8 EB)
JFS (512 Bytes tamaño bloque)	2^{63} (8 EB)	2^{49} (512 TB)
JFS (4 kB tamaño bloque)	2^{63} (8 EB)	2^{52} (4 PB)
NFSv2 (lado del cliente)	2^{31} (2 GB)	2^{63} (8 EB)
NFSv3 (lado del cliente)	2^{63} (8 EB)	2^{63} (8 EB)

Cuadro A.2: Tamaño máximo de los sistemas de archivos (formato en disco)

Atención

Límites del kernel de Linux

La tabla describe los límites del formato en disco. El tamaño máximo de un archivo y un sistema de archivos para que puedan ser procesados correctamente por el kernel no ha de superar los siguientes límites (en el kernel 2.4.x):

- *Sistemas de 32 bits:* Los archivos y los dispositivos de bloque no pueden ser mayores de 2 Tb (2^{41} byte). No obstante, LVM permite combinar varios dispositivos de bloque para procesar sistemas de archivos por encima del límite de 2 Tb.
- *Sistemas de 64 bits:* Los archivos y los sistemas de archivos pueden tener un tamaño de hasta 8 Eb (2^{63} byte), siempre que el hardware lo soporte.

Atención

Información adicional

Cada proyecto de sistema de archivos descrito arriba tiene su propia página web en la que puede encontrar más información y listas de correo, así como FAQs.

<http://e2fsprogs.sourceforge.net/ext2.html>

<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/>

Un completo tutorial sobre sistemas de archivos en Linux se encuentra en *IBM developerWorks*:

<http://www-106.ibm.com/developerworks/library/l-fs.html>

Una comparación entre los distintos sistemas de archivos journaling en Linux se encuentra en un artículo de Juan I. Santos Florido en *Linuxgazette*: <http://www.linuxgazette.com/issue55/florido.html>.

Se puede encontrar un detallado trabajo sobre LFS en Linux en la página de Andreas Jaeger: http://www.suse.de/~aj/linux_lfs.html.

Listas de control de acceso (ACLs) en Linux

Este capítulo le proporciona información sobre el trasfondo y las funciones de las ACLs POSIX para sistemas de archivos Linux. En él aprenderá cómo se amplía el concepto tradicional de permisos para sistemas de archivos por medio de las ACLs (*Access Control Lists*) y qué ventajas ofrece este concepto.

¿Por qué ACLs?	560
Definiciones	561
Funcionamiento de las ACLs	561
El futuro de las ACLs	571

¿Por qué ACLs?

Atención

POSIX ACLs

La expresión "POSIX ACL" sugiere que se trata de un auténtico estándar de la familia POSIX (*Portable Operating System Interface*). Por diversos motivos se retiraron los borradores de los estándares POSIX 1003.1e y POSIX 1003.2c. No obstante, las ACLs en muchos sistemas operativos de tipo UNIX se basan en estos documentos. La implementación de ACLs de sistemas de archivos descrita en este capítulo está basada en el contenido de estos dos documentos que se pueden consultar en la siguiente URL:

<http://wt.xpilot.org/publications/posix.1e/>

Atención

De manera tradicional, un objeto en Linux está asociado a tres grupos de permisos. Estos grupos reflejan los permisos de escritura (w), lectura (r) y ejecución (x) para las tres clases de usuarios: propietario del archivo ((ingl. *owner*)), grupo ((ingl. *group*)) y el resto ((ingl. *other*)). Además es posible definir los bits *set user id*, *set group id* y *sticky*. Puede obtener información adicional sobre este tema en el apartado *Derechos de usuario* del *Manual de usuario*.

Para la mayoría de los casos que se dan en la práctica, este escueto concepto es más que suficiente. En el caso de escenarios complejos o aplicaciones más avanzadas, hasta ahora los administradores de sistemas debían echar mano de distintos trucos para evitar las limitaciones del concepto de permisos tradicional.

Las ACLs intervienen en las situaciones en las que el concepto tradicional de permisos para archivos resulta insuficiente. Éstas permiten asignar permisos a determinados usuarios o grupos, incluso cuando estos permisos no coinciden con los del propietario del archivo o su grupo.

Las listas de control de acceso son una característica del kernel de Linux y actualmente están soportadas por ReiserFS, Ext2, Ext3, JFS y XFS. Con su ayuda es posible llevar a la práctica complejos escenarios sin que sea necesario implementar complicados modelos de permisos a nivel de aplicaciones.

Para ilustrar las ventajas de las listas de control de acceso puede tomarse el ejemplo de un servidor Windows que va a ser reemplazado por un servidor Linux. Algunas de las estaciones de trabajo conectadas seguirán funcionando con Windows. El sistema Linux, por su parte, proporciona a los clientes Windows servicios de servidor de archivos y de impresión por medio de Samba.

Samba soporta las listas de control de acceso, por lo que los permisos de usuarios pueden ser configurados tanto en el servidor Linux como en Windows (sólo Windows NT o superior) a través de una interfaz gráfica de usuario. La herramienta winbindd permite incluso definir permisos para usuarios que sólo existen en el dominio Windows y no disponen de cuenta de usuario en el servidor Linux. En la parte del servidor, las listas de control de acceso pueden ser editadas con `getfacl` y `setfacl`.

Definiciones

Clases de usuarios El sistema tradicional de permisos POSIX reconoce tres *clases* de usuarios para la asignación de permisos en el sistema de archivos: Propietario (ingl. *owner*), grupo (ingl. *group*) y el resto de usuarios (ingl. *other*). Para cada clase de usuario se pueden definir otros tres bits de permisos ((ingl. *permission bits*)) para el derecho de lectura (*r*), de escritura (*w*) y de ejecución (*x*). La sección *Derechos de usuario* del *Manual de Usuario* le ofrece una introducción al concepto de usuarios en Linux.

Access ACL Los permisos de acceso de usuarios y grupos a cualquier objeto del sistema (archivos y directorios) se definen a través de las access ACLs (*ACLs de acceso*).

Default ACL Las default ACLs (*ACLs predeterminadas*) sólo pueden aplicarse a directorios y definen los permisos que un objeto del sistema "hereda" del directorio superior al ser creado.

Entrada ACL Una ACL está formada por una serie de entradas ACL (ingl. *ACL entries*). Una entrada ACL consta de un tipo (ver la Tabla B.1 en la página siguiente), un indicador del usuario o el grupo al que se refiere la entrada, y los permisos en sí. En algunos tipos de entrada, el indicador para el usuario o el grupo está vacío.

Funcionamiento de las ACLs

En la siguiente sección se describirán la estructura básica de una ACL y sus características. La relación entre las ACLs y el concepto tradicional de permisos en el sistema de archivos Linux se explicará por medio de varios gráficos. Dos ejemplos le servirán para conocer la sintaxis correcta de una ACL y crear sus propias listas de control de acceso. Finalmente, se describirá el método usado por el sistema operativo para evaluar las ACLs.

Estructura de las entradas ACL

Las ACLs pueden dividirse fundamentalmente en dos clases. Una ACL *estándar* consiste exclusivamente en las entradas de tipo *owner* (propietario), *owning group* (grupo propietario) y *other* (otros) y coincide con los bits de permisos tradicionales para archivos y directorios. Una ACL *extendida* (ingl. *extended*) contiene además una entrada *mask* (máscara) y puede incluir varias entradas del tipo *named user* (usuario identificado por el nombre) y *named group* (grupo identificado por el nombre). La tabla B.1 ofrece un resumen de los distintos tipos de entradas ACL.

Tipo	Formato en texto
owner	user::rwx
named user	user:name:rwx
owning group	group::rwx
named group	group:name:rwx
mask	mask::rwx
other	other::rwx

Cuadro B.1: Resumen de tipos de entrada ACL

Los permisos definidos en las entradas *owner* y *other* siempre tienen vigencia. Excepto la entrada *mask*, el resto de entradas (*named user*, *owning group* y *named group*) pueden estar activadas o bien enmascaradas. Si se han definido permisos tanto en las entradas mencionadas en primer lugar como en las máscara, tendrán validez. Los permisos que sólo han sido definidos en la máscara o en la propia entrada, no tienen validez. El siguiente ejemplo ilustra este mecanismo (véase la Tabla B.2):

Tipo	Formato en texto	Permisos
named user	user:jane:r-x	r-x
mask	mask::rw-	rw-
Válidos:		r--

Cuadro B.2: Enmascaramiento de permisos de acceso

Entradas ACL y bits de permiso

Los siguientes gráficos ilustran respectivamente las posibles variantes de una ACL estándar y una extendida (ver Fig. B.1 y B.2). Las figuras están divididas en tres bloques. A la izquierda aparece la descripción del tipo de entrada ACL, en el medio un ejemplo de ACL y a la derecha los bits de permiso tal y como los muestra el comando `ls -l`.

En ambos casos, los permisos correspondientes al *owner class* han sido asignados a la entrada ACL *owner*. Asimismo, la asignación de permisos *other class* a la correspondiente entrada ACL es siempre la misma. En cambio, la asignación de permisos *group class* varía según el caso.

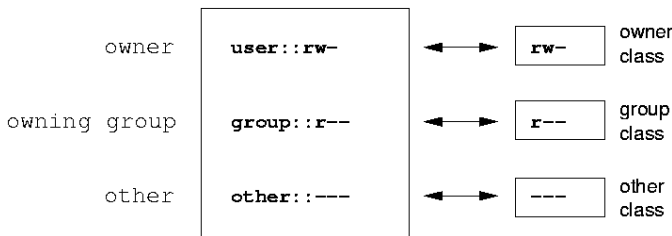


Figura B.1: ACL estándar: entradas ACL y bits de permiso

- En el caso de una ACL estándar (sin entrada *mask*), los permisos de la *group class* se asignan a la entrada ACL *owning group* (ver Fig. B.1).
- En el caso de una ACL extendida (con entrada *mask*), los permisos de la *group class* se asignan a la entrada *mask* (ver Fig. B.2).

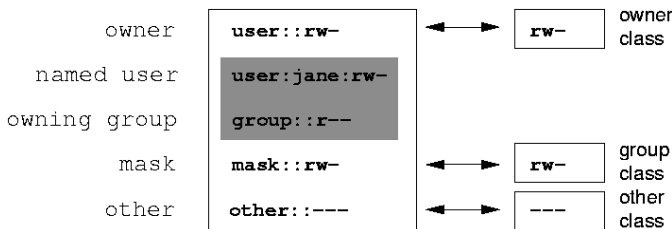


Figura B.2: ACL extendida: entradas ACL y bits de permiso

Este tipo de asignación garantiza la correcta interacción de aplicaciones con y sin soporte ACL. Los permisos de acceso definidos mediante los bits de permiso constituyen el límite para las opciones de configuración avanzadas que pueden realizarse vía ACL. Todos los permisos que no están reflejados aquí no han sido definidos en la ACL o no tienen vigencia. Si los bits de permiso se modifican, esto también se refleja en la ACL correspondiente y viceversa.

Un directorio con access ACL

Por medio del siguiente ejemplo, se explicará en tres pasos el funcionamiento de una access ACL:

- Crear un objeto del sistema (aquí un directorio)
 - Cambios en la ACL
 - Utilización de máscaras
1. Antes de crear un directorio, puede emplear el comando `umask` para definir qué permisos de acceso han de estar enmascarados desde el principio.

```
umask 027
```

`umask 027` define los permisos de cada grupo de usuarios como se describe a continuación: el propietario del archivo posee todos los permisos (0), el grupo al que pertenece el propietario no tiene permiso de escritura sobre el archivo (2) y el resto de usuarios carece de cualquier permiso sobre el archivo (7). Los números se leen como una máscara de bits. Puede obtener más información sobre `umask` en la página del manual correspondiente (`man umask`).

```
mkdir mydir
```

Se ha creado el directorio `mydir` que ha obtenido los derechos definidos por medio de `umask`. Puede comprobar si todos los permisos han sido asignados correctamente con el comando:

```
ls -dl mydir
drwxr-x--- ... tux projekt3 ... mydir
```


2. Una vez que se ha informado sobre el estado inicial de la ACL, añádale una nueva entrada de usuario y otra de grupo.

```
getfacl mydir

# file: mydir
# owner: tux
# group: projekt3
user::rwx
group::r-x
other:---
```

La salida del comando `getfacl` refleja exactamente la correspondencia entre bits de permiso y entradas ACL descrita en el apartado [Entradas ACL y bits de permiso](#) en la página 563. Las primeras tres líneas de la salida de comando designan el nombre, propietario y grupos pertenecientes del directorio. Las tres líneas siguientes contienen las tres entradas ACL *owner*, *owning group* y *other*. En conjunto, el comando `getfacl` en el caso de esta ACL estándar no le ofrece ninguna información que no hubiese obtenido también con el comando `ls`.

Su primera intervención en la ACL consiste en asignar a un nuevo usuario `jane` y a un nuevo grupo `djungle` permisos de lectura, escritura y ejecución.

```
setfacl -m user:jane:rwx,group:djungle:rwx mydir
```

La opción `-m` le ordena a `setfacl` modificar la ACL actual. El siguiente argumento indica qué entradas ACL serán modificadas (muchas están separadas entre sí por comas). Finalmente tiene que introducir el nombre del directorio para el que tendrán validez estos cambios.

La ACL resultante se muestra con el comando `getfacl`.

```
getfacl mydir

# file: mydir
# owner: tux
# group: projekt3
user::rwx
user:jane:rwx
group::r-x
group:djungle:rwx
mask::rwx
other:---
```

Además de las entradas para el usuario *jane* y el grupo *djungle* creadas por usted, se ha generado una entrada *mask*. Esta entrada *mask* se crea automáticamente para reducir todas las entradas de *group class* a un denominador común. Además, *setfacl* adapta automáticamente las entradas *mask* a las opciones que usted modifique (siempre que no haya desactivado esta función con *-n*). *mask* define los permisos de acceso máximos que tienen validez para todas las entradas de la *group class*. Entre éstas se incluyen *named user*, *named group* y *owning group*. Los bits de permiso de *group class* mostrados al ejecutar `ls -dl mydir` equivalen a la entrada *mask*.

```
ls -dl mydir
drwxrwx---+ ... tux projekt3 ... mydir
```

En la primera columna de la salida aparece un signo *+* que hace referencia a una ACL *extendida*.

- Según la salida del comando `ls`, los permisos de la entrada *mask* incluyen también permiso de escritura. Normalmente, estos bits de permiso también indicarían que el *owning group* (aquí: *projekt3*) tendría asimismo derechos de escritura para el directorio *mydir*. No obstante, los permisos de acceso realmente válidos para el *owning group* consisten en la intersección de los permisos definidos para el *owning group* y *mask*, es decir, *r-x* en nuestro ejemplo (ver la tabla B.2 en la página 562). Aquí tampoco se han modificado los permisos de *owning group* después de añadir las entradas ACL.

La entrada *mask* puede modificarse con *setfacl* o con *chmod*.

```
chmod g-w mydir
ls -dl mydir

drwxr-x---+ ... tux projekt3 ... mydir

getfacl mydir

# file: mydir
# owner: tux
# group: projekt3
user::rwx
user:jane:rwx          # effective: r-x
group::r-x
group:djungle:rwx      # effective: r-x
mask::r-x
other::---
```

Después de haber retirado el permiso de escritura a la *group class* por medio del comando `chmod`, la salida del comando `ls` ya le indica que los bits de *mask* han sido adaptados en consecuencia a través del comando `chmod`. Como se puede ver, el único que posee permiso de escritura sobre el directorio `mydir` es el propietario. Esto se ve aún más claramente en la salida del comando `getfacl`. Además, `getfacl` añade a cada entrada un comentario informando de que los bits de permiso realmente válidos no son los definidos inicialmente, ya que la entrada *mask* se encarga de filtrarlos. Por supuesto, se puede volver a en cualquier momento al estado original con el comando `chmod` correspondiente:

```
chmod g+w mydir
ls -dl mydir

drwxrwx---+ ... tux projekt3 ... mydir

getfacl mydir

# file: mydir
# owner: tux
# group: projekt3
user::rwx
user:jane:rwx
group::r-x
group:djungle:rwx
mask::rwx
other::---
```

Directorios con ACLs predeterminadas

Los directorios pueden ser equipados con un tipo especial de ACLs, las ACLs predeterminadas. Éstas definen los derechos que heredan todos los subobjetos de estos directorios en el momento de su creación. La ACL predeterminada tiene vigencia tanto sobre subdirectorios como sobre archivos.

Efecto de una ACL predeterminada

Los permisos de acceso en la ACL predeterminada son heredados de forma distinta por archivos y subdirectorios:

- Un subdirectorio hereda la ACL predeterminada del directorio superior como propia default ACL y además como access ACL.
- Un archivo hereda la ACL predeterminada como propia access ACL.

Todas las llamadas del sistema (ingl. *system calls*) que crean objetos del sistema utilizan un parámetro `mode`. Este parámetro se encarga de definir los permisos de acceso sobre el nuevo objeto del sistema:

- Si el directorio superior carece de ACL predeterminada, los permisos resultantes son los introducidos en el parámetro `mode` menos los permisos asignados en `umask`.
- Si existe una ACL predeterminada para el directorio superior, se asignan al objeto los bits de permiso resultantes de la intersección de los permisos del parámetro `mode` y de los que contiene la ACL predeterminada, sin tener en cuenta `umask`.

ACLs predeterminadas en la práctica

Los tres ejemplos siguientes ilustran las ACLs predeterminadas y describen las operaciones más importantes que pueden efectuarse en directorios:

- Crear una ACL predeterminada para un directorio ya existente.
 - Crear un subdirectorio en un directorio con ACL predeterminada.
 - Crear un archivo en un directorio con ACL predeterminada.
1. A continuación se añade una ACL predeterminada al directorio `mydir` ya existente:

```
setfacl -d -m group:djungle:r-x mydir
```

La opción `-d` del comando `setfacl` hace que `setfacl` realice las siguientes modificaciones en (opción `-m`) en la ACL predeterminada.

Observe el resultado de este comando detenidamente:

```
getfacl mydir
```

```
# file: mydir
# owner: tux
# group: projekt3
user::rwx
```

```
user:jane:rwx
group::r-x
group:djungle:rwx
mask::rwx
other:---
default:user::rwx
default:group::r-x
default:group:djungle:r-x
default:mask::r-x
default:other:---
```

La salida de `getfacl` contiene tanto la access ACL como la ACL predeterminada. Todas las líneas que comienzan por `default` forman la ACL predeterminada. Aunque en el comando `setfacl` usted sólo había indicado una entrada para el grupo `djungle` en la ACL predeterminada, `setfacl` ha copiado automáticamente el resto de entradas de la access ACL para construir una ACL predeterminada válida. Las ACLs predeterminadas no influyen de manera directa en los permisos de acceso, sino que sólo tienen efecto durante la creación de objetos del sistema. En términos de herencia, sólo se tiene en cuenta la ACL predeterminada del directorio superior.

2. En el siguiente ejemplo cree con `mkdir` un subdirectorio en `mydir` que "heredará" la ACL predeterminada.

```
mkdir mydir/mysubdir
getfacl mydir/mysubdir

# file: mydir/mysubdir
# owner: tux
# group: projekt3
user::rwx
group::r-x
group:djungle:r-x
mask::r-x
other:---
default:user::rwx
default:group::r-x
default:group:djungle:r-x
default:mask::r-x
default:other:---
```

Como era de esperar, el subdirectorio recién creado `mysubdir` tiene los permisos de la ACL predeterminada ACL del directorio superior.

La access ACL de `mysubdir` es una réplica exacta de la ACL predeterminada de `mydir`. Lo mismo sucede con la ACL predeterminada, que a su vez se pasará a los subobjetos de este directorio.

3. Ahora cree un archivo en el directorio `mydir` por medio de `touch`:

```
touch mydir/myfile
ls -l mydir/myfile

-rw-r-----+ ... tux projekt3 ... mydir/myfile

getfacl mydir/myfile

# file: mydir/myfile
# owner: tux
# group: projekt3
user::rw-
group::r-x      # effective:r--
group:djungle:r-x  # effective:r--
mask::r--
other::---
```

Lo más importante de este ejemplo es que `touch` pasa el parámetro `mode` con un valor de `0666`, lo que significa que los nuevos archivos se crean con permisos de lectura y escritura para todas las clases de usuario, a no ser que existan otras restricciones por parte de `umask` o de la ACL predeterminada (ver la sección *Efecto de una ACL predeterminada* en la página 567).

En nuestro ejemplo esto significa que todos los permisos que no están incluidos en `mode` serán eliminados de las entradas ACL correspondientes. Aunque no se ha eliminado ningún permiso de la entrada ACL de *group class*, la entrada *mask* ha sido adaptada para que los bits de permiso definidos por `mode` no sean enmascarados.

De este modo se garantiza que un compilador, por ejemplo, pueda funcionar sin problemas con ACLs. Puede crear archivos con permisos de acceso restringidos y a continuación marcarlos como ejecutables. El mecanismo `mask` se ocupa de que sólo los usuarios y grupos adecuados obtengan los derechos que les han sido asignados en la ACL predeterminada.

Evaluación de una ACL

Una vez explicado el funcionamiento de las herramientas de configuración más importantes de las ACLs, a continuación se describe brevemente el algoritmo

de evaluación al que se somete cualquier proceso o aplicación antes de que se le proporcione acceso a un objeto del sistema protegido por ACLs.

Las entradas ACL son analizadas en el siguiente orden: *owner*, *named user*, *owning group* o *named group* y *other*. El acceso se regula a través de la entrada que mejor se ajuste al proceso.

El mecanismo se complica cuando un proceso pertenece a más de un grupo, ya que potencialmente podrá ajustarse a varias entradas *group*. En este caso se selecciona una de las entradas adecuadas con los permisos requeridos. Para el resultado final "acceso autorizado" es irrelevante cuál de estas entradas ha sido seleccionada. Si ninguna de las entradas *group* apropiadas contiene los permisos correctos, se selecciona una cualquiera que provocará el resultado final "acceso denegado".

El futuro de las ACLs

Como se ha mencionado en los apartados anteriores, las ACLs permiten implementar complejos escenarios de permisos que cumplen a la perfección los requisitos de las aplicaciones más actuales. El concepto tradicional de permisos y las ACLs pueden combinarse de forma muy hábil.

No obstante, algunas aplicaciones importantes carecen todavía de soporte para ACLs. Sobre todo en el campo de los programas de copias de seguridad, no existe (con la excepción del archivador *stör*) ningún programa que pueda garantizar el mantenimiento total de las ACLs.

Los comandos de archivos básicos (*cp*, *mv*, *ls*, etc.) soportan las ACLs. En cambio, numerosos editores y administradores de archivos (ej. Konqueror) carecen de soporte ACL. Así, las ACLs todavía se pierden al copiar archivos con Konqueror. Al procesar con un editor un archivo que contenga una *access ACL*, el que la *access ACL* se mantenga o no tras finalizar el proceso de edición depende del modo *backup* del editor utilizado:

- Si el editor escribe los cambios en el archivo original, la *access ACL* se mantiene.
- Si el editor crea un nuevo archivo que recibe el nombre del antiguo archivo al finalizar los cambios, es posible que se pierdan las ACL a no ser que el editor las soporte.

Cuanto más extendido esté el soporte de ACLs en las aplicaciones, mejor se podrán explotar estas funciones.

Truco

Información adicional

Puede encontrar información detallada (en inglés) sobre las ACLs en las siguientes URLs

http://sdb.suse.de/en/sdb/html/81_acl.html

<http://acl.bestbits.at/>

así como en las páginas del manual de página del manual de `getfacl` (`man 1 getfacl`), página del manual de `acl` (`man 5 acl`) y página del manual de `setfacl` (`man 1 setfacl`).

Truco

Página man de e2fsck

E2FSCK(8)

E2FSCK(8)

NAME

e2fsck - check a Linux second extended file system

SYNOPSIS

```
e2fsck [ -pacnyrdfvstFSV ] [ -b superblock ] [ -B block-size ] [ -l|-L bad_blocks_file ] [ -C fd ] [ -j external-journal ] [ device ]
```

DESCRIPTION

e2fsck is used to check a Linux second extended file system (e2fs). E2fsck also supports ext2 filesystems containing a journal, which are also sometimes known as ext3 filesystems.

device is the special file corresponding to the device (e.g /dev/hdc1).

OPTIONS

-a This option does the same thing as the -p option. It is provided for backwards compatibility only; it is suggested that people use -p option whenever possible.

-b superblock

Instead of using the normal superblock, use an alternative superblock specified by superblock. This option is normally used when the primary superblock has been corrupted. The location of the backup superblock is dependent on the filesystem's blocksize. For filesystems with 1k blocksizes, a backup superblock can be found at block 8193; for filesystems with 2k blocksizes, at block 16384; and for 4k blocksizes, at block 32768.

Additional backup superblocks can be determined by using the mke2fs program using the -n option to print out where the superblocks were created. The -b option to mke2fs, which specifies blocksize of the filesystem must be specified in order for the superblock locations that are printed out to be accurate.

If an alternative superblock is specified and the filesystem is not opened read-only, e2fsck will make sure that the primary superblock is updated appropriately upon completion of the filesystem check.

-B blocksize

Normally, e2fsck will search for the superblock at various different block sizes in an attempt to find the appropriate block size. This search can be fooled in some cases. This option forces e2fsck to only try locating the superblock at a particular blocksize. If the superblock is not found, e2fsck will terminate with a fatal error.

-c This option causes e2fsck to run the badblocks(8) program to find any blocks which are bad on the filesystem, and then marks them as bad by adding them to the bad block inode.

-C This option causes e2fsck to write completion information to the specified file descriptor so that the progress of the filesystem check can be monitored. This option is typically used by programs which are running e2fsck. If the file descriptor specified is 0, e2fsck will print a completion bar as it goes about its business. This requires that e2fsck is running on a video console or terminal.

-d Print debugging output (useless unless you are debugging e2fsck).

-f Force checking even if the file system seems clean.

-F Flush the filesystem device's buffer caches before beginning. Only really useful for doing e2fsck time trials.

-j external-journal

Set the pathname where the external-journal for this filesystem can be found.

-l filename

Add the blocks listed in the file specified by

filename to the list of bad blocks. The format of this file is the same as the one generated by the badblocks(8) program.

- L filename
Set the bad blocks list to be the list of blocks specified by filename. (This option is the same as the -l option, except the bad blocks list is cleared before the blocks listed in the file are added to the bad blocks list.)

- n Open the filesystem read-only, and assume an answer of 'no' to all questions. Allows e2fsck to be used non-interactively. (Note: if the -c, -l, or -L options are specified in addition to the -n option, then the filesystem will be opened read-write, to permit the bad-blocks list to be updated. However, no other changes will be made to the filesystem.)

- p Automatically repair ("preen") the file system without any questions.

- r This option does nothing at all; it is provided only for backwards compatibility.

- s This option will byte-swap the filesystem so that it is using the normalized, standard byte-order (which is i386 or little endian). If the filesystem is already in the standard byte-order, e2fsck will take no action.

- S This option will byte-swap the filesystem, regardless of its current byte-order.

- t Print timing statistics for e2fsck. If this option is used twice, additional timing statistics are printed on a pass by pass basis.

- v Verbose mode.

- V Print version information and exit.

- y Assume an answer of 'yes' to all questions; allows e2fsck to be used non-interactively.

EXIT CODE

The exit code returned by e2fsck is the sum of the following conditions:

- 0 - No errors
- 1 - File system errors corrected
- 2 - File system errors corrected, system should

be rebooted if file system was mounted
4 - File system errors left uncorrected
8 - Operational error
16 - Usage or syntax error
128 - Shared library error

SIGNALS

The following signals have the following effect when sent to e2fsck.

SIGUSR1

This signal causes e2fsck to start displaying a completion bar. (See discussion of the -C option.)

SIGUSR2

This signal causes e2fsck to stop displaying a completion bar.

REPORTING BUGS

Almost any piece of software will have bugs. If you manage to find a filesystem which causes e2fsck to crash, or which e2fsck is unable to repair, please report it to the author.

Please include as much information as possible in your bug report. Ideally, include a complete transcript of the e2fsck run, so I can see exactly what error messages are displayed. If you have a writeable filesystem where the transcript can be stored, the script(1) program is a handy way to save the output of e2fsck to a file.

It is also useful to send the output of dumpe2fs(8). If a specific inode or inodes seems to be giving e2fsck trouble, try running the debugfs(8) command and send the output of the stat(1u) command run on the relevant inode(s). If the inode is a directory, the debugfs dump command will allow you to extract the contents of the directory inode, which can sent to me after being first run through uuen code(1).

Always include the full version string which e2fsck displays when it is run, so I know which version you are running.

AUTHOR

This version of e2fsck was written by Theodore Ts'o <tytso@mit.edu>.

SEE ALSO

mke2fs(8), tune2fs(8), dumpe2fs(8), debugfs(8)

E2fsprogs version 1.25 September 2001

E2FSCK(8)

Página man de reiserfsck

REISERFSCK(8)

REISERFSCK(8)

NAME

reiserfsck - check a Linux Reiserfs file system

SYNOPSIS

```
reiserfsck [ -afprVy ] [ --check | --fix-fixable |
--rebuild-sb | --rebuild-tree | --clean-attributes ] [ -j
| --journal-device device ] [ --no-journal-available ] [
-z | --adjust-file-size ] [ -S | --scan-whole-partition ]
[ -l | --logfile filename ] [ -n | --nolog ] [ -q |
--quiet ] device
```

DESCRIPTION

Reiserfsck searches for a Reiserfs filesystem on a device, replays any necessary transactions, and either checks or repairs the file system.

device is the special file corresponding to the device or partition (e.g /dev/hdXX for IDE disk partition or /dev/sdXX for SCSI disk partition).

OPTIONS

--check

This default action checks file system consistency and reports but does not repair any corruption that it finds. This option may be used on a read-only file system mount. The --check option exits with status 0 to indicate that no corruption was found. Otherwise, reiserfsck returns 1 to indicate corruption that can be fixed with --fix-fixable and 2 to indicate corruption that requires --rebuild-tree.

--fix-fixable

This option recovers certain kinds of corruption

that do not require rebuilding the entire file system tree (`--rebuild-tree`). Normally you only need this option if the `--check` option reports "corruption that can be fixed with `--fix-fixable`". This includes: zeroing invalid data-block pointers, correcting `st_size` and `st_blocks` for directories, and deleting invalid directory entries.

`--rebuild-sb`

This option recovers the superblock on a Reiserfs partition. Normally you only need this option if mount reports "read_super_block: can't find a reiserfs file system" and you are sure that a Reiserfs file system is there.

`--rebuild-tree`

This option rebuilds the entire file system tree using leaf nodes found on the device. Normally you only need this option if the `--check` option reports "corruption that can be fixed only during `--rebuild-tree`". You are strongly encouraged to make a backup copy of the whole partition before attempting the `--rebuild-tree` option.

`--clean-attributes`

This option cleans reserved fields of Stat-Data items.

`--journal-device device, -j device`

This option supplies the device name of the current file system journal. This option is required when the journal resides on a separate device from the main data device (although it can be avoided with the expert option `--no-journal-available`).

`--adjust-file-size, -z`

This option causes reiserfsck to correct file sizes that are larger than the offset of the last discovered byte. This implies that holes at the end of a file will be removed. File sizes that are smaller than the offset of the last discovered byte are corrected by `--fix-fixable`.

`--logfile filename, -l filename`

This option causes reiserfsck to report any corruption it finds to the specified log file rather than `stderr`.

`--nolog, -n`

This option prevents reiserfsck from reporting any kinds of corruption.

`--quiet, -q`

This option prevents reiserfsck from reporting its rate of progress.

-a, -p These options are usually passed by fsck -A during the automatic checking of /etc/fstab partitions. For compatibility, these options simply cause reiserfsck to print information about the specified file system. No checks are performed. When it is set - reiserfsck assumes that it is called by fsck -A, provides some information about the specified filesystem and exits.

-V This option prints the reiserfsprogs version and exit.

-r, -p, -y
These options are ignored.

-V, -f prints version and exits

EXPERT OPTIONS

DO NOT USE THESE OPTIONS UNLESS YOU KNOW WHAT YOU ARE DOING. WE ARE NOT RESPONSIBLE IF YOU LOSE DATA AS A RESULT OF THESE OPTIONS.

--no-journal-available

This option allows reiserfsck to proceed when the journal device is not available. This option has no effect when the journal is located on the main data device. NOTE: after this operation you must use reiserfstune to specify a new journal device.

--scan-whole-partition, -S

This option causes --rebuild-tree to scan the whole partition, not only used space on the partition.

EXAMPLE OF USING

1. You think something may be wrong with a reiserfs partition on /dev/hda1 or you would just like to perform a periodic disk check.

2. Run reiserfsck --check --logfile check.log /dev/hda1. If reiserfsck --check exits with status 0 it means no errors were discovered.

3. If reiserfsck --check exits with status 1 (and reports about fixable corruptions) it means that you should run reiserfsck --fix-fixable --logfile fixable.log /dev/hda1.

4. If reiserfsck --check exits with status 2 (and reports about fatal corruptions) it means that you need to run reiserfsck --rebuild-tree. If reiserfsck --check fails in some way you should also run reiserfsck --rebuild-tree,

but we also encourage you to submit this as a bug report.

5. Before running `reiserfsck --rebuild-tree`, please make a backup of the whole partition before proceeding. Then run `reiserfsck --rebuild-tree --logfile rebuild.log /dev/hda1`.

6. If the `--rebuild-tree` step fails or does not recover what you expected, please submit this as a bug report. Try to provide as much information as possible and we will try to help solve the problem.

EXIT CODE

`reiserfsck` uses the following exit codes:

- 0 - No errors
- 1 - File system errors corrected
- 2 - File system errors corrected, system should be rebooted if file system was mounted
- 4 - File system errors left uncorrected
- 8 - Operational error
- 16 - Usage or syntax error

AUTHOR

This version of `reiserfsck` has been written by Vitaly Fertman <vitaly@namesys.com> and Vladimir Saveliev <vs@namesys.com>.

BUGS

There are likely to be some bugs. Please report bugs to the ReiserFS mail-list <reiserfs-list@namesys.com>.

TODO

Faster recovering, signal handling, i/o error handling, return reasonable exit codes, etc.

SEE ALSO

`mkreiserfs(8)`, `debugreiserfs(8)`, `reiserfstune(8)`

Reiserfsprogs-3.6.2

January 2002

REISERFSCK(8)

La licencia pública general GNU (GPL)

Esta traducción de la GPL se ofrece con el fin de mejorar el entendimiento de la licencia. No se trata de una traducción oficial o jurídicamente reconocida.

La *Free Software Foundation* (FSF) no edita esta traducción y tampoco la ha reconocido como reemplazo oficial de la versión original en inglés (disponible en <http://www.gnu.org/copyleft/gpl.html>). Los traductores de la licencia no pueden garantizar que la traducción reproduzca exactamente las definiciones jurídicas. Para estar seguro que las actividades que esté planificando estén permitidas bajo la licencia GNU-GPL, consulte el original en inglés.

La *Free Software Foundation* ruega no utilizar esta traducción como licencia oficial para los programas que Usted escriba. En su lugar, acompañe su software con la versión original inglesa de la licencia.

This is a translation of the GNU General Public License into Spanish. This translation is distributed in the hope that it will facilitate understanding, but it is not an official or legally approved translation.

The Free Software Foundation is not the publisher of this translation and has not approved it as a legal substitute for the authentic GNU General Public License. The translation has not been reviewed carefully by lawyers, and therefore the translator cannot be sure that it exactly represents the legal meaning of the GNU General Public License. If you wish to be sure whether your planned activities are permitted by the GNU General Public License, please refer to the authentic English version.

The Free Software Foundation strongly urges you not to use this translation as the official distribution terms for your programs; instead, please use the authentic English version published by the Free Software Foundation.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Se permite a todo el mundo la copia y distribución de copias literales de este documento de licencia, pero no se permite su modificación.

Esta traducción no reemplaza la versión original en inglés de la GPL en el sentido jurídico.

Preámbulo

Las licencias que cubren la mayor parte del software están diseñadas para quitarle a usted la libertad de compartirlo y modificarlo. Por el contrario, la Licencia Pública General GNU pretende garantizarle la libertad de compartir y modificar software libre—para asegurar que el software es libre para todos sus usuarios. Esta Licencia Pública General se aplica a la mayor parte del software de la Free Software Foundation y a cualquier otro programa cuyos autores se comprometen a utilizarla. (Alguna parte del software de la Free Software Foundation está cubierto por la Licencia Pública General GNU para Librerías). Usted también la puede aplicar a sus programas.

Cuando hablamos de software libre, estamos refiriéndonos a la libertad, no al precio. Nuestras Licencias Públicas Generales están diseñadas para asegurarnos de que tenga la libertad de distribuir copias de software libre (y cobrar por ese servicio si quiere), que reciba el código fuente o que pueda conseguirlo si lo quiere, que pueda modificar el software o usar fragmentos de él en nuevos programas libres, y que sepa que puede hacer todas estas cosas.

Para proteger sus derechos necesitamos algunas restricciones que prohíban a cualquiera negarle a usted estos derechos o pedirle que renuncie a ellos. Estas restricciones se traducen en ciertas obligaciones que le afectan si distribuye copias del software, o si lo modifica.

Por ejemplo, si distribuye copias de uno de estos programas, sea gratuitamente, o a cambio de una contraprestación, debe dar a los receptores todos los derechos que tiene. Debe asegurarse de que ellos también reciben, o pueden conseguir, el código fuente. Y debe mostrarles estas condiciones de forma que conozcan sus derechos.

Protegemos sus derechos con la combinación de dos medidas: (1) ponemos el software bajo copyright y (2) le ofrecemos esta licencia, que le da permiso legal para copiar, distribuir y/o modificar el software.

También, para la protección de cada autor y la nuestra propia, queremos asegurarnos de que todo el mundo comprende que no se proporciona ninguna garantía para este software libre. Si el software es modificado por cualquiera y éste a su vez lo distribuye, queremos que sus receptores sepan que lo que tienen no es el original, de forma que cualquier problema introducido por otros no afecte a la reputación de los autores originales.

Por último, cualquier programa libre está constantemente amenazado por patentes sobre el software. Queremos evitar el riesgo de que los redistribuidores de un programa libre individualmente obtengan patentes, haciendo el programa propietario a todos los efectos. Para prevenir esto, hemos dejado claro que cualquier patente debe ser concedida para el uso libre de cualquiera, o no ser concedida en absoluto.

Los términos exactos y las condiciones para la copia, distribución y modificación se exponen a continuación.

Licencia pública general GNU

Términos y condiciones para la copia, distribución y modificación

0. Esta Licencia se aplica a cualquier programa u otra obra que contenga un aviso colocado por el propietario del copyright diciendo que puede ser distribuido bajo los términos de esta Licencia Pública General. En adelante, "Programa" se referirá a cualquier programa u obra de esta clase y "una obra basada en el Programa" se referirá bien al Programa o a cualquier obra derivada de este según la ley de copyright. Esto es, una obra que contenga el programa o una porción de este, bien en forma literal o con modificaciones y/o traducido en otro lenguaje. Por lo tanto, la traducción está incluida sin limitaciones en el término "modificación". Cada propietario de una licencia será tratado como "usted".

Cualquier otra actividad que no sea la copia, distribución o modificación no está cubierta por esta Licencia, está fuera de su ámbito. El acto de ejecutar el Programa no está restringido, y los resultados del Programa están cubiertos únicamente si sus contenidos constituyen una obra basada en el Programa, independientemente de haberlo producido mediante la ejecución del programa. Que esto se cumpla, depende de lo que haga el programa.

1. Usted puede copiar y distribuir copias literales del código fuente del Programa, tal y como lo recibió, por cualquier medio, supuesto que de forma adecuada y bien visible publique en cada copia un anuncio de copyright adecuado y una renuncia de garantía, mantenga intactos todos los anuncios que se refieran a esta Licencia y a la ausencia de garantía, y proporcione a cualquier otro receptor del programa una copia de esta Licencia junto con el Programa.

Puede cobrar un precio por el acto físico de transferir una copia, y puede a su elección ofrecer garantía a cambio de unos honorarios.

2. Usted puede modificar su copia o copias del Programa o cualquier porción de él, formando de esta manera una obra basada en el Programa, y copiar y distribuir esa modificación u obra bajo los términos del apartado 1 anterior, siempre que además cumpla las siguientes condiciones:

- a) Debe procurar que los ficheros modificados incluyan notificaciones destacadas manifestando que los ha cambiado y la fecha de cualquier cambio.
- b) Usted debe procurar que cualquier obra que distribuya o publique, que en todo o en parte contenga o sea derivada del Programa o de cualquier parte de él, sea licenciada como un todo, sin cargo alguno para terceras partes bajo los términos de esta Licencia.
- c) Si el programa modificado lee normalmente órdenes interactivamente cuando al ejecutarse, debe hacer que cuando comience su ejecución para ese uso interactivo de la forma más habitual, muestre o escriba un mensaje que incluya un anuncio de copyright y un anuncio de que no se ofrece ninguna garantía (o por el contrario que sí se ofrece garantía) y que los usuarios pueden redistribuir el programa bajo estas condiciones, e indicando al usuario cómo ver una copia de esta licencia. (Excepción: si el propio programa es interactivo pero normalmente no muestra ese anuncio, no está obligado a que su obra basada en el Programa muestre ningún anuncio).

Estos requisitos se aplican a la obra modificada como un todo. Si algunas secciones claramente identificables de esa obra no están derivadas del Programa, y pueden razonablemente ser consideradas como obras independientes y separados por sí mismas, entonces esta Licencia y sus términos no se aplican a esas partes cuando sean distribuidas como trabajos separados. Pero cuando distribuya esas mismas secciones como partes de un todo que es una obra basada en el Programa, la distribución de ese todo debe cumplir los términos de esta Licencia, cuyos permisos para otros licenciarios se extienden al todo completo, y por lo tanto a todas y cada una de sus partes, con independencia de quién la escribió.

Por lo tanto, no es intención de este apartado reclamar derechos u oponerse a sus derechos sobre obras escritas enteramente por usted; sino que la intención es ejercer el derecho de controlar la distribución de obras derivadas o colectivas basadas en el Programa.

Además, el simple hecho de reunir otro trabajo no basado en el Programa con el Programa (o con un trabajo basado en el Programa) en un medio de almacenamiento o en un medio de distribución no hace que dicho trabajo entre dentro del ámbito cubierto por esta Licencia.

3. Usted puede copiar y distribuir el Programa (o una obra basada en él, según se especifica en la Sección 2) en forma de código objeto o ejecutable bajo los términos de las Secciones 1 y 2 anteriores mientras cumpla además una de las siguientes condiciones:

- a) Acompañarlo con el código fuente completo correspondiente en formato legible para un ordenador, que debe ser distribuido bajo los términos de las Secciones 1 y 2 anteriores en un medio utilizado habitualmente para el intercambio de programas, o
- b) Acompañarlo con una oferta por escrito, válida durante al menos tres años, por un coste no mayor que el de realizar físicamente la distribución del fuente, de proporcionar a cualquier tercera parte una copia completa en formato legible para un ordenador del código fuente correspondiente, que será distribuido bajo las condiciones descritas en las Secciones 1 y 2 anteriores, en un medio utilizado habitualmente para el intercambio de programas, o
- c) Acompañarlo con la información que usted recibió referida al ofrecimiento de distribuir el código fuente correspondiente. (Esta opción se permite sólo para la distribución no comercial y sólo si usted recibió el programa como código objeto o en formato ejecutable con una oferta de este tipo, de acuerdo con la Sección b anterior).

Se entiende por código fuente de un trabajo a la forma preferida de la obra para hacer modificaciones sobre este. Para una obra ejecutable, se entiende por código fuente completo todo el código fuente para todos los módulos que contiene, más cualquier fichero asociado de definición de interfaces, más los guiones utilizados para controlar la compilación e instalación del ejecutable. Como excepción especial el código fuente distribuido no necesita incluir nada que sea distribuido normalmente (ya sea en formato fuente o binario) con los componentes fundamentales (compilador, kernel y similares) del sistema operativo en el cual funciona el ejecutable, a no ser que el propio componente acompañe al ejecutable.

Si la distribución del ejecutable o del código objeto se realiza ofreciendo acceso a una copia desde un lugar designado, entonces se considera el ofrecimiento del

acceso para copiar el código fuente del mismo lugar como distribución del código fuente, incluso aunque terceras partes no estén obligadas a copiar el fuente junto al código objeto.

4. No puede copiar, modificar, sublicenciar o distribuir el Programa excepto como está expresamente permitido por esta Licencia. Cualquier intento de copiar, modificar sublicenciar o distribuir el Programa de otra forma es inválido, y hará que cesen automáticamente los derechos que le proporciona esta Licencia. En cualquier caso, las partes que hayan recibido copias o derechos bajo esta Licencia no verán sus Licencias canceladas, mientras esas partes continúen cumpliendo totalmente la Licencia.

5. No está obligado a aceptar esta licencia, ya que no la ha firmado. Sin embargo, no hay nada más que le proporcione permiso para modificar o distribuir el Programa o sus trabajos derivados. Estas acciones están prohibidas por la ley si no acepta esta Licencia. Por lo tanto, si modifica o distribuye el Programa (o cualquier trabajo basado en el Programa), está indicando que acepta esta Licencia para poder hacerlo, y todos sus términos y condiciones para copiar, distribuir o modificar el Programa o trabajos basados en él.

6. Cada vez que redistribuya el Programa (o cualquier trabajo basado en el Programa), el receptor recibe automáticamente una licencia del licenciario original para copiar, distribuir o modificar el Programa, de forma sujeta a estos términos y condiciones. No puede imponer al receptor ninguna restricción más sobre el ejercicio de los derechos aquí garantizados. No es usted responsable de hacer cumplir esta licencia por terceras partes.

7. Si como consecuencia de una resolución judicial o de una alegación de infracción de patente o por cualquier otra razón (no limitada a asuntos relacionados con patentes) se le imponen condiciones (ya sea por mandato judicial, por acuerdo o por cualquier otra causa) que contradigan las condiciones de esta Licencia, ello no le exime de cumplir las condiciones de esta Licencia. Si no puede realizar distribuciones de forma que se satisfagan simultáneamente sus obligaciones bajo esta licencia y cualquier otra obligación pertinente entonces, como consecuencia, no puede distribuir el Programa de ninguna forma. Por ejemplo, si una patente no permite la redistribución libre de derechos de autor del Programa por parte de todos aquellos que reciban copias directa o indirectamente a través de usted, entonces la única forma en que podría satisfacer tanto esa condición como esta Licencia sería evitar completamente la distribución del Programa.

Si cualquier porción de este apartado se considera no válido o imposible de cumplir bajo cualquier circunstancia particular ha de cumplirse el resto y la sección por entero ha de cumplirse en cualquier otra circunstancia.

No es el propósito de este apartado inducirle a infringir ninguna patente ni ningún otro derecho de propiedad o impugnar la validez de ninguna de dichas reclamaciones. Este apartado tiene el único propósito de proteger la integridad del sistema de distribución de software libre, que se realiza mediante prácticas de licencia pública. Mucha gente ha hecho contribuciones generosas a la gran variedad de software distribuido mediante ese sistema con la confianza de que el sistema se aplicará consistentemente. Será el autor/donante quien decida si quiere distribuir software mediante cualquier otro sistema y una licencia no puede imponer esa elección.

Este apartado pretende dejar completamente claro lo que se cree que es una consecuencia del resto de esta Licencia.

8. Si la distribución y/o uso de el Programa está restringido en ciertos países, bien por patentes o por interfaces bajo copyright, el poseedor del copyright que coloca este Programa bajo esta Licencia puede añadir una limitación explícita de distribución geográfica excluyendo esos países, de forma que la distribución se permita sólo en o entre los países no excluidos de esta manera. En ese caso, esta Licencia incorporará la limitación como si estuviese escrita en el cuerpo de esta Licencia.

9. La Free Software Foundation puede publicar versiones revisadas y/o nuevas de la Licencia Pública General de tiempo en tiempo. Dichas versiones nuevas serán similares en espíritu a la presente versión, pero pueden ser diferentes en detalles para considerar nuevos problemas o situaciones.

Cada versión recibe un número de versión que la distingue de otras. Si el Programa especifica un número de versión de esta Licencia que se aplica a ella y a "cualquier versión posterior", tiene la opción de seguir los términos y condiciones, bien de esa versión, bien de cualquier versión posterior publicada por la Free Software Foundation. Si el Programa no especifica un número de versión de esta Licencia, puede escoger cualquier versión publicada por la Free Software Foundation.

10. Si usted desea incorporar partes del Programa en otros programas libres cuyas condiciones de distribución son diferentes, escriba al autor para pedirle permiso. Si el software tiene copyright de la Free Software Foundation, escriba a la Free Software Foundation: algunas veces hacemos excepciones en estos casos.

Nuestra decisión estará guiada por el doble objetivo de preservar la libertad de todos los derivados de nuestro software libre y promover el que se comparta y reutilice el software en general.

Ausencia de garantía

11. YA QUE EL PROGRAMA SE LICENCIA LIBRE DE CARGAS, NO SE OFRECE NINGUNA GARANTÍA SOBRE EL PROGRAMA, HASTA LO PERMITIDO POR LAS LEYES APLICABLES. EXCEPTO CUANDO SE INDIQUE LO CONTRARIO POR ESCRITO, LOS POSEEDORES DEL COPYRIGHT Y/OTRAS PARTES PROVEEN EL PROGRAMA "TAL Y COMO ESTÁ", SIN GARANTÍA DE NINGUNA CLASE, YA SEA EXPRESA O IMPLÍCITA, INCLUYENDO, PERO NO LIMITÁNDOSE A, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD Y APTITUD PARA UN PROPÓSITO PARTICULAR. TODO EL RIESGO EN CUANTO A LA CALIDAD Y FUNCIONAMIENTO DEL PROGRAMA LO ASUME USTED. SI EL PROGRAMA SE COMPROBARA QUE ESTÁ DEFECTUOSO, USTED ASUME EL COSTO DE TODO SERVICIO, REPARACIÓN O CORRECCIÓN QUE SEA NECESARIO.

12. EN NINGÚN CASO, A NO SER QUE SE REQUIERA POR LAS LEYES APLICABLES O SE ACUERDE POR ESCRITO, PODRÁ NINGÚN POSEEDOR DE COPYRIGHT O CUALQUIER OTRA PARTE QUE HAYA MODIFICADO Y/O REDISTRIBUIDO EL PROGRAMA, SER RESPONSABLE ANTE USTED POR DAÑOS O PERJUICIOS, INCLUYENDO CUALQUIER DAÑO GENERAL, ESPECIAL, INCIDENTAL O CONSECUENTE DEBIDO AL USO O LA IMPOSIBILIDAD DE PODER USAR EL PROGRAMA (INCLUYENDO PERO NO LIMITÁNDOSE A LA PÉRDIDA DE DATOS O LA PRODUCCIÓN DE DATOS INCORRECTOS O PÉRDIDAS SUFRIDAS POR USTED O POR TERCERAS PARTES O LA IMPOSIBILIDAD DEL PROGRAMA DE OPERAR JUNTO A OTROS PROGRAMAS), INCLUSO SI EL POSEEDOR DEL COPYRIGHT U OTRA PARTE HA SIDO AVISADO DE LA POSIBILIDAD DE TALES DAÑOS.

FIN DE TÉRMINOS Y CONDICIONES

Anexo: Cómo aplicar estos términos a sus nuevos programas propios.

Si usted desarrolla un nuevo Programa, y quiere que sea del mayor uso posible para el público en general, la mejor forma de conseguirlo es convirtiéndolo en software libre que cualquiera pueda redistribuir y cambiar bajo estos términos.

Para hacerlo, añada los siguientes avisos al programa. Lo más seguro es añadirlos al principio de cada fichero fuente para comunicar lo más efectivamente

posible la ausencia de garantía. Además cada fichero debería tener al menos la línea de "copyright" y una indicación del lugar donde se encuentra la notificación completa.

una línea para indicar el nombre del programa y una rápida idea de lo que hace

Copyright (C) 19yy *nombre del autor*

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307, USA.

En castellano:

Este programa es software libre; usted puede redistribuirlo y/o modificarlo bajo los términos de la Licencia Pública General GNU tal y como está publicada por la Free Software Foundation; ya sea la versión 2 de la Licencia o (a su elección) cualquier versión posterior.

Este programa se distribuye con la esperanza de que sea útil, pero SIN NINGUNA GARANTÍA; ni siquiera la garantía implícita de COMERCIALIZACIÓN o APTITUD PARA UN PROPÓSITO ESPECÍFICO. Vea la Licencia Pública General GNU para más detalles.

Usted debería haber recibido una copia de la Licencia Pública General junto con este programa. Si no ha sido así, escriba a la Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

Añada también información sobre cómo contactar con usted mediante correo electrónico y postal.

Si el programa es interactivo, haga que muestre un pequeño anuncio como el siguiente, cuando comience a funcionar en modo interactivo:

Gnomovision versión 69, Copyright (C) 19yy *nombre del autor*

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'. This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

En castellano:

Gnomovision no ofrece ABSOLUTAMENTE NINGUNA GARANTÍA; para más detalles escriba 'show w'. Esto es software libre, y se le invita a redistribuirlo bajo ciertas condiciones. Escriba 'show c' para más detalles.

Los comandos hipotéticos 'show w' y 'show c' deberían mostrar las partes adecuadas de la Licencia Pública General. Por supuesto, los comandos que use pueden llamarse de cualquier otra manera. Podrían incluso ser pulsaciones del ratón o elementos de un menú—lo que sea apropiado para su programa).

También debería conseguir que el empresario (si trabaja como programador) o su centro académico, si es el caso, firme una "renuncia de copyright" para el programa, si es necesario. A continuación se ofrece un ejemplo, cambie los nombres:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program 'Gnomovision' (which makes passes at compilers) written by James Hacker.

Signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

En castellano:

Yoyodyne, Inc. con la presente renuncia a cualquier interés de derechos de copyright con respecto al programa 'Gnomovision' (que hace pasadas a compiladores) escrito por Pepe Programador.

firma de Pepito Grillo, 1 de abril de 1989

Pepito Grillo, Presidente de Asuntillos Varios.

Esta Licencia Pública General no permite incorporar su programa a programas propietarios. Si su programa es una librería de subrutinas, puede considerar más útil el permitir el enlazado de aplicaciones propietarias con la librería. Si este es el caso, use la Licencia Pública General GNU para Librerías en lugar de esta Licencia.

Índice alfabético

Simbolos

/etc/inittab	296
/etc/profile	<i>véase</i> bash, /etc/profile
/etc/resolv.conf	272
sistema X Window	<i>véase</i> X11
YaST	
- Imprimir	134

A

Actualización	43
- /etc/skel	49
- profile	49
Actualización del sistema	43
Advertencia Virus	16
Apache	51
- Squid	489
APM	
- Parámetros del kernel	50
Apple	
- Netatalk	457
Aquid	
- SARG	493
Archivo de configuración	
- stcany.upp	176
Archivos	
- Buscar	51
- grandes	555
- Imprimir	147, 150, 169, 172
archivos de configuración	
- dhcpd.conf	388
Archivos de configuración	330
- .lptions	167, 171
- /boot/grub/menu.lst	78
- /etc/conf.modules	<i>véase</i>
/etc/modules.conf	
- /etc/foomatic/filter.conf	54

- /etc/grub.conf	84
- /etc/init.d/boot	50
- /etc/lilo.conf	88
- /etc/logfiles	50
- /etc/modules.conf	261
- /etc/xinetd.d/cups-lpd	201
- /etc/xml/catalog	54
- /etc/xml/suse-catalog.xml	54
- cups	
- lptions	171
- cupsd.conf	163
- exports	384
- host.conf	333
- HOSTNAME	336
- ifroute-*	337
- lpd.conf	146
- lpd.perms	146
- lpdfilter	151, 153
- mime.convs	165
- modules.conf	141
- named.conf	340
- nsd.conf	336
- nsswitch.conf	334, 367
- pam_unix2.conf	366
- printcap	146, 151, 152, 186
- resolv.conf	331
- Rutas	337
- slapd.conf	356
- squid.conf	489
- squidguard.conf	492
Archivos de registro	268
Arrancar	295
- con disquete	23
- Bootmanager	76
- con disquetes	21

- con el CD2	24
- Concepto	75
- Gestor de arranque	76
- GRUB	77-86
- initial ramdisk	273
- LILO	73
- Métodos	16
- Proceso	74
Arranque	573
- Concepto	295
- El ordenador se cuelga <i>véase</i> BIOS, Virus Protection	

ASCII	
- Codificación	181
autoexec.bat	301
autofs	51

B

bash	
- /etc/profile	267
bind	333
BIND	339
BIOS	
- Virus Protection	16
Boot	573
Booting	577
Bootloader	73
- GRUB	77
Bootmanager	73
- GRUB	76
- LILO	76
- Windows NT	76
build	63
Busmouse	103

C

Cargador de arranque	
- GRUB	73, 77
- LILO	73
CD-ROM	
- se traba	25
CD-ROM-ATAPI se traba	25
Check	577
Clock-Chip	106
Comando	
- ulimit	270
Compose	<i>véase</i> Disposición del teclado, Compose
Comprar PC	282
Conexión a redes	311
Conexión telefónica	
- smpppd	470
Configuración	

- Cambiar	304
- Cargador de arranque	
- GRUB	77
- LILO	88
- Imprimir	134-139
- IPv6	328
- Kernel	255-264
- manual	329
- Red	326
- Samba	449-456
- SSH	502
- X11	102

Configurar servicios del sistema	<i>véase</i> sysconfig

Consola	
- virtual	289
Consolas virtuales	289
Controladora ATA-RAID <i>véase</i> Hardware, Controladora Promise	
Controladora GDT RAID5 ... <i>véase</i> ICP Vortex	
Controladora ICP Vortex	
- Instalación falla	15
Controladora Promise	<i>véase</i> Hardware, Controladora Promise
Controladora RAID	
- ATA <i>véase</i> Hardware, Controladora Promise	
Cortafuegos	496
- filtro de paquetes	496
- Squid y	486
- SuSEfirewall2	496, 499
- configurar	499
Crash	573, 577
Crear usuario	
- Problemas	336
cron	268
Cuelgue	573

D

Daemons	
- lpd	145
depmod	260
Desinstalar	
- GRUB	93
- LILO	92, 93
- Linux	93
- Squid	479
DHCP	387-391
- Asignación estática de direcciones	390
- Configuración del servidor	388
- Paquetes	387
Direcciones	
- IP	316

- MAC	316
Direcciones IP	
- IPv6	
· Prefijos	323
direcciones IP	
- masquerading	496
Direcciones IP	316, 318
- Clases de red	316
- IPv6	320
· Estructura	322
- Routing	316
Direcciones IPv6	
- Máscaras de red	324
Disco duro IDE	
- Controladora ATA-RAID	<i>véase</i>
Hardware, Controladora Promise	
Disposición del teclado	
- Compose	290
Disquete	
- Arrancar de	75
- Formatear	22
Disquete de arranque	23, 50, 75, 88
- Crear con rawrite	21
- Generar con dd	22
Disquete de rescate	283
Distribución del teclado	289
DNS	319, 339
- Análisis de problemas	340
- archivos de zona	344
- Forwarding	340
- Iniciar	339
- Logging	343
- Mail Exchanger	320
- Opciones	341
- Squid	479
- Zonas	343
DNS:Resolución de nombres inversa	347
Domain Name System	339
Dominio	331
E	
2fsck	573
Editor de niveles de ejecución	303
El ordenador se cuelga	<i>véase</i> BIOS, Virus
Protection	
Emacs	<i>véase</i> Software, Emacs
Emergencia	
- Sistema de rescate	283
enrutado	
- masquerading	496
Enrutamiento	
- Rutas	337
Entorno de desarrollo	63

ES-NIC	339
Exportar	383

F

fdisk	94
FHS	<i>véase</i> Sistema de ficheros, FHS
Ficheros	
- grandes	556
- Permisos sobre ficheros	270
Ficheros Core	270
ficheros de configuración	
- SuSEfirewall2	499
Ficheros de configuración	
- squid.conf	486
filtro de paquetes	496
FireGL	9
Firewall	496
Frecuencia horizontal	104
Frecuencia vertical	104
free	271
Fuentes	
- Compilar	62

G

Gestor de arranque	73
- GRUB	76
- LILO	76
- Windows NT	76
Ghostscript	173-177
- Controlador	130
GNOME	
- Compilar	55
GNU Emacs	<i>véase</i> Software, Emacs
GPL	581
Gráficos	
- 3D	120
· Controladores	120
· Diagnóstico	122
· Probar	122
· Resolución de problemas	122
· SaX2	121
· Soporte	120
· Soporte de instalación	123
· Troubleshooting	122
- id	121
- Tarjetas FireGL	9
GRUB	73, 77
- /etc/grub.conf	84
- Bootpassword	85
- Desinstalar	93
- Menú de arranque	78
- Nombres de dispositivos	79
- Nombres de particiones	79

- Resolución de problemas	86
- Shell GRUB	84
- Troubleshooting	86
Grupos	
- Cambio de nombre	51
gs	<i>véase</i> Ghostscript
H	
hardn_suse	52
Hardware	
- Controladora Promise	45
- Laptop	209
- Portátil	209
host.conf	334
hosts	332, 333
Hotplug	203, 328
- Cámaras	206
- Dispositivos de almacenamiento	205
- Dispositivos de red	206
- en Linux	204
- PCI	206
- PCMCIA	206
- Ratones	206
- Teclado	206
- USB	205
I	
I18N	291
Identifier	115
Importar	382
Imprimir	125
- a2ps	177
- Archivos	147, 150, 169, 172
- Búsqueda de errores	
· CUPS	167
- Búsqueda de fallos	
· Red	196
- Cola de impresión	126, 134, 138
· controlar	148–150
· Herramientas	147–151
· Opciones	170
- Colas de impresión	
· administrar	169–173
· color	134
· Eliminar trabajos de impresión	148, 150
· en red	172
· Estado	148, 150, 170, 172
· raw	152, 167
· remotas	149–150
- Configuración	134
· YaST	134
· CUPS	162–163
· Lprng y lpdfilter	145
· Puertos	140–145
- Controlador	130–133
- Controladores Ghostscript	130
- CUPS	134, 161–168
· Búsqueda de errores	167
· OpenOffice.org	166
· Resolución de problemas	172
- cups-lpd	184
- dúplex	155
- Desarrollo	126–127
- desde aplicaciones	140, 168
- Filtro de impresión	
· Búsqueda de errores	160–161
· configurar	153
· editar	153–154
· Ejemplo	154
· lpdfilter	151–161
- footmatic-filters	54
- Fundamentos	126–129
- Ghostscript	173
· Controlador	130–131
- Impresora GDI	131–133
· Configuración	159
· soportadas	133
- Impresoras de red	164
- Impresoras soportadas	129
- IPP	161
- Línea de comandos	147
- Línea de comandos, desde la	169
- Lenguajes de impresión	126
· ASCII	126
· ESC	126
· PCL	126
· PostScript	126
- lpc	148–149
- lpq	150
- lpr	147, 150
- LPRng	54, 135
· Comandos	147
- lprsetup	145
- Páginas de cubierta	139
- PPD	163
- Procesamiento	165
- Protocolos	186
- Red	183
· Búsqueda de fallos	196
- Requisitos	129
- Resolución de problemas	150
· CUPS	172
- Servidor CUPS	184
- Servidor de impresión	183
- Servidor de impresión dedicado	183

- Servidor de red CUPS	184	- Registro	518
- Servidor IPP	184	- Replay	510
- Servidor LPD	184	- Session Key	510
- Spooler		- Sincronización del reloj	517
· lpd	145–146	- Soporte PAM	527–528
- Trabajos		- Ticket	509
· Procesamiento	165	Kernel	255
- Trabajos de impresión		- Compilación	255
· eliminar	148, 150, 170	- Configuración	257
· Eliminar	172	- Daemon	261
· Estado	148, 150, 170	- Instalar	263
inetd	53	- Módulos	259
Info (info)	270	· Compilar	262
Información del sistema	279	· depmod	260
init	296	· insmod	260
- Añadir scripts	301	· modinfo	261
- scripts	299	· modprobe	260, 261
Initial ramdisk (initrd)	273	· parport	140
inittab	296	· rmmmod	260
insmod	260	- Module Loader	261
Instalación		Kernel too big	262
- en modo texto, con YaST	8	kerneld	261
- FTP	18	L	
- GRUB	77	L10N	291
- Kernel	263	LAN	326
- NFS	18	Laptop	209
- Paquetes	55	LDAP	351–376
- PCMCIA	219	- Árbol de directorios	354
- Red como fuente	18	- Añadir datos	361
Instalar		- Access Control Information	360
- LILO	92	- Access Control Lists	357
Internet		- Administrar grupos	373
- smpppd	470	- Administrar usuarios	373
IrDA	244	- Borrar datos	365
iso-8859	118	- Cliente LDAP YaST	366
J		- Cliente LDAP de YaST	
jade	<i>véase SGML, openjade</i>	· Módulo	367
K		· Plantillas	367
Kerberos	508	- Configuración de servidor	356
- Authenticator	509	- Examinar datos	365
- Clave maestra	519	- Kerberos y LDAP	529–532
- Configuración de clientes	521–524	- ldapadd	361
- Configuración de SSH	528	- ldapdelete	365
- Credential	509	- ldapmodify	364
- Host principal	526	- ldapsearch	365
- Instalación y administración	515–532	- Modificar datos	364
- KDC	518–521	Lector CD-ROM	
- LDAP y Kerberos	529–532	- Soporte en Linux	24
- Mutual Authentication	510	Licencia	581
- Principal	510, 520	Lightweight Directory Access Protocol ..	<i>véase</i>
- Realm	515, 519	LDAP	
		LILO	73, 87

- Configuración	88
- Desinstalar	93
- Fundamentos	87
- Instalar	92
Linux	
- Actualización	43
- Desinstalar	93
- Update	43
Linux Standard Base	266
linuxrc	278
Local Area Network	<i>véase LAN</i>
locate	51
Logfiles	<i>véase Archivos de registro, véase Archivos de registro</i>
Logical Volume Manager ..	<i>véase YaST, Gestor Volúmenes Lógicos</i>
Logitech	103
lprsetup	145
LSB	<i>véase Linux Standard Base</i>
LSB (Linux Standard Base)	
- Instalar paquetes	54
lsmod	261
LVM	<i>véase YaST, LVM</i>
M	
Módulo	
- Cargar	280
- hwinfo	260
- Parámetros	281
Módulo kernel	
- Tarjeta de red	326
Módulos	
- Manejo	260
MacOS	457
Manpages	<i>véase Páginas man</i>
masquerading	496
- configuración con SuSEfirewall2 ..	499
Masquerading	496
MBR	74, 88, <i>véase Master Boot Record</i>
Memoria	
- Memoria de trabajo	271
mkinitrd	277
Modeline	117
modinfo	261
Modo	
- Gráfico <i>véase Pantalla gráfica de SuSE, desactivar</i>	
Modo gráfico . <i>véase Pantalla gráfica de SuSE, desactivar</i>	
modprobe	260
Monitor	104
mount	383
mountd	383

Multi_key *véase Disposición del teclado, Compose*

N

Name Service Cache Daemon	336
Name Service Switch	334
Nameserver	333
NAT	<i>véase masquerading</i>
Netatalk	457
NetBIOS	448
- Servicio de nombres	448
NetWare	<i>véase Novell NetWare</i>
Network File System	<i>véase NFS</i>
Network Information Service	<i>véase NIS</i>
networks	332
NFS	382
NFS cliente	382
NFS servidor	382
nfsd	383
NIS	377
- autofs	51
- Clientes	379
Nivel de ejecución	296
Notebook	
- IrDA	244
nVidia	52

O

OpenGL	120
- Controladores	120
- Probar	122
OpenOffice.org	
- Imprimir	
- Cups	166
OpenSSH	<i>véase SSH</i>

P

Páginas man	270
Pantalla gráfica	
- Desactivar	16
Pantalla virtual	115
paquete	
- a2ps	177
- aaa_base	268
- alsa-devel	55
- apache	401
- apache-devel	402
- apache-doc	402
- apache-example-pages	402
- apache2	401
- apache2-devel	402
- apache2-doc	402
- apache2-example-pages	402

- apache2-mod_php4	416
- apache2-mod_python	417
- apache2-prefork	401
- apache2-worker	401
- apmd	231, 233
- binutils	257
- build	63, 64
- bzip	52
- bzip2	52
- cups	135, 163, 169
- cups-client	135, 168, 169
- cups-drivers	54, 135, 163
- cups-drivers-stp	135, 163, 166
- cups-libs	135
- dhcpcd	388
- docbook-toys	53
- emacs	272, 273
- emacs-auctex	273
- emacs-el	273
- emacs-info	273
- emacs-nox	273
- emacs-x11	273
- exports	383
- fhs	266
- find-locate	51
- footmatic-filters	54, 135
- ftpdir	51, 266
- gcc	257
- Ghostscript	135
- ghostscript-fonts-std	136
- ghostscript-library	136
- ghostscript-x11	136
- gimp-devel	55
- glibc	63
- glibc-devel	257
- glibc-info	294
- gnuserv	273
- gv	173, 181
- howtoen	493
- howtoes	499
- ipxrip	468
- irda	144, 245
- isapnp	50
- jade_dsl	53
- kbd	50
- KDE	135
- kdelibs-devel	55
- kernel-source	257, 261, 262
- libcinfo	334
- libgimpprint	136
- libz	52
- logrotate	268
- lpdfilter	135, 151
- lprng	135, 145
- LPRng	146
- lvm	50
- mesa	123
- mod_perl	402
- mod_php4	401, 402, 416
- mod_php4-core	416
- mod_python	402, 417
- ncpfs	467, 468
- netatalk	457, 463
- NVIDIA_GLX	52
- NVIDIA_kernel	52
- openjade	53
- openldap	52
- openldap2	52
- pcmcia	211, 220
- pcmcia-cardinfo	220
- pcmcia-modules	221
- pmtools	238
- popt	52
- popt-devel	52
- postgres	45
- psgml	273
- psutils	154, 178
- radvd	329
- rpm	52, 63
- rpm-devel	52
- rzsz	53
- samba	449
- Samba	135
- samba-client	164, 166
- sdb_en	49
- squidgrd	492
- su1	52
- sudo	52
- SuSEfirewall2	162, 496
- syslinux	23, 96
- sysvinit	63
- tcl	258
- tk	258
- tpctl	231
- wget	61
- wine	135
- xf86	258
- XFree86	123
- xntp-doc	394
- yast2-trans-*	52
- yast2-trans-cs	52
- yast2-trans-de	52
- yast2-trans-es	52
- yudit	119
- zlib	52
- zlib-devel	52

Paquetes	
- Compilar	62
- construir	53
- Construir	63
- Desinstalar	55
- Formato de paquetes	54
- Gestor de paquetes	54
- Instalar	55
- LSB	54
Parámetros del kernel	
- APM	50
Partición	
- Swap	27
Particionador	<i>véase</i> YaST, Particionador
Particionar	
- Experto	26
- fdisk	94
- Tabla de partición	74
PCI	206
PCMCIA	206, 210, 328
- Administrador de tarjetas	211
- Configuración	212
- Instalación	219
- IrDA	244
- Módem	213
- RDSI	213
- Resolución de errores	215
- SCPM	214
- SCSI	214
- Tarjetas de red	213
- Utilidades	220
PGP	55
pine	51
Portátil	209
Portátiles	
- PCMCIA	328
- SCPM	222
portmap	383
PostgreSQL	
- Update	45
PostScript	
- Reformatear	178–181
Primera instalación	
- Arrancar con disquete	23
- Arrancar con el CD2	24
- Disquetes de arranque	21
- Futuros métodos de arranque	16
- Generar disquete de arranque bajo un sistema tipo Unix	22
- linuxrc	10
- Pantalla de bienvenida	8
Probar PC	282
Programar	
- Ficheros Core	270
Programas	
- Compilar	62
Protocolos	
- ICMP	313
- IGMP	313
- IPP	161
- TCP/IP	312
- UDP	313
Proxy	
- Squid	474
- transparente	485
- Ventajas	474
Puerto	
- IrDA	144
- paralelo	140–142
- serie	145
- USB	142–144
R	
Ramdac	106
Ratón	
- Bus	103
- HiTablet	103
- Logitech	103
- Logitech (MouseMan)	103
- Microsoft	103
- MM-Serie	103
- Mouse Systems	103
- pine	51
- PS/2	103
- Tipo	103
Red	
- Archivos de configuración	330
- Asignación dinámica de direcciones	387
- Configuración	326
- IPv6	328
- Dirección base	318
- Direcciones IP	316
- DNS	319
- Imprimir	164
- Imprimir en	183
- Kerberos	508
- Localhost	318
- Routing	316
Redes	311
- Máscaras de red	316
- Routing	316
reiserfsck	577
Remote Login	50
Rescue-System	283
Resolución de nombres	

- NIS	333
Resolución de pantalla	115
resolv.conf	<i>véase /etc/resolv.conf</i>
rmmod	260
Routing	316, 337
- estático	337
- Máscaras de red	316
- Routes	337
RPC-Mount-Daemon	383
RPC-NFS-Daemon	383
RPC-Portmapper	383
RPM	54
- Parches	57
- rpmnew	55
- rpmorig	55
- rpmsave	55
- Version 4	53
rpmbuild	53, 54
Runlevel	296
- cambiar	298

S

Samba	448–456
- Configuración del servidor	449
- Niveles de seguridad	452
- Recursos compartidos (ingl. <i>shares</i>)	450
SCPM	214, 222
- Administrar perfiles	224
- Configurar	224
Script	
- init.d	
· inetd	337
· network	337
· nfsserver	337
· portmap	337
· sendmail	337
· ypbind	337
· ypserv	337
- lpdfilter	
· guess	152
· modify_resolvconf	332
Scripts de arranque	
- init.d	336
Sector de arranque	74
Seguridad	532
- Cortafuegos	496
- Firewall	496
- Squid	475
- SSH	502–508
serie	
- xap	119
Servidor de nombres	331, 339
- BIND	339

Servidor FTP	51
- Configurar	266
Servidor HTTP	<i>véase Apache</i>
- Configurar	267
SGML	
- openjade	53
Sistema de archivos	547–557
- Access ACL	561, 564
- ACL predeterminada	561, 567
- Default ACL	561, 567
- Ext2	548–549
- Ext3	549–551
- JFS	552–553
- Limitaciones	555
- ReiserFS	551–552
- Selección	548
- soportados	554–555
- Términos	547
- XFS	553–554
Sistema de colas	125
Sistema de ficheros	
- FHS	266
- Reconstruir	573
- TeX	266
Sistema de impresión	<i>véase Sistema de colas</i>
Sistema de rescate	283
- Iniciar	285
- Preparativos	284
- Uso	287
Sistema X Window	99
Sistemas de archivos	
- Access Control Lists	559–572
- Listas de control de acceso	559–572
SMB	<i>véase Samba</i>
smpppd	470
Soft-RAID	<i>véase YaST, Soft-RAID</i>
Software	
- Emacs	272
Soporte de instalación	
- Tarjetas gráficas 3D	123
Squid	474
- Apache	489
- Arrancar	478
- Cachear objetos	476
- cachemgr.cgi	489
- Caches	475
- Calamaris	492
- Características	474
- Control de acceso	483, 489
- Cortafuegos	486
- CPU	478
- Discos duros	476
- DNS	479

- Estadísticas	489
- Permisos	483
- Proxy transparente	485
- Proxy-Cache	474
- RAM	477
- Seguridad	475
- squidGuard	491
- Tamaño del caché	477
SSH	502-508
- Autenticación	506
- scp	504
- sftp	504
- ssh-agent	507
- sshd	504
Stick USB	
- Arrancar de	76
SuSE	265
SuSEconfig	304
SuSEConfig	304
SuSE Linux	265
- Distribución del teclado	289
- Instalación	278
- Particularidades	265
- Sistema de rescate	283
Swap-Partición	27
sx	53
sysconfig	50
/etc/sysconfig	304
System	
- Update	43
System is too big	262

T

Tarjeta de red	
- Prueba	326
TCP/IP	312, 313
- Modelo de capas	313
TCP/Servicios	312
Teclas de ratón	104
Texinfo	270
Tkinfo (tkinfo)	270
TrueType	<i>véase</i> X11, TrueType

U

UDP	<i>véase</i> TCP
ugidd	385
ulimit	270
Unicode	119
Update	43
USB	205
Usuarios	
- Cambio de nombre	51

V

Variable de entorno	
- ACPI_BUTTON_LID	240
- ACPI_BUTTON_POWER	240
- APMD_AC	233
- APMD_BATTERY	233
- CUPS_SERVER	162
- HOME	44
- HTTPD_SEC_PUBLIC_HTML	409
- PATH	3, 412
- QUERY_STRING	412
Variables de entorno	
- CUPS_SERVER	162
Virus Protection ..	<i>véase</i> BIOS, Virus Protection

W

whois	320
Windows	448
- NT Bootmanager	76
- SMB	448
Windows NT	
- Bootmanager	76
- Gestor de arranque	76

X

X	<i>véase</i> X11
X Window System	99
X11	99
- Configuración	102
- Monitores	104
- Ratón	103
- Servidor X	106
- Teclado	104
- Driver	116
- Font	117
- Fuentes	117
- mkfontdir	117
- Optimización	111
- Tarjetas gráfica	106
- TrueType-Font	117
- ttmkfdir	117
X11R6.4	100
xf86config	102
XF86Config	102
- Clocks	115
- Depth	115
- Device	113-115
- Files	112
- InputDevice	112
- modeline	115
- Modeline	113
- Modes	113, 115, 116
- Monitor	113, 114, 116

- Screen	113, 114
- ServerFlags	112
- ServerLayout	113
- Subsection	
· Display	115
- Virtual	115
XFree86	100
- Historia	100
xinetd	53
XInfo (xinfo)	270
XML	
- Catálogo	54
- openjade	53
Y	
YaST	50

- Actualización en línea mediante la consola	71
- Clientes NIS	379
- Distribución del teclado	67
- Editor de niveles de ejecución	303
- Editor sysconfig	306
- Gestor Volúmenes Lógicos	32
- Logical Volume Manager	32
- LVM	32
- Modo texto	67
- ncurses	67
- Particionador	31
- Soft-RAID	39
Yellow Pages	<i>véase</i> NIS
yudit	119