SUSE LINUX

Manual de administración

Edición 2005

Dirija sus comentarios y sugerencias a `documentation@suse.de`.

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

Traducción: Inés Pozo Muñoz

Redacción: Jörg Arndt, Antje Faber, Berthold Gunreben, Roland Haidl, Jana Jaeger, Edith Parzefall, Inés Pozo Muñoz, Thomas Rölz, Thomas Schraitle

Diseño: Manuela Piotrowski, Thomas Schraitle

Composición: DocBook-XML, LaTeX

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

Bienvenido

Enhorabuena por su nuevo sistema operativo LINUX y gracias por haber optado por SUSE LINUX 9.3. El precio de compra incluye asistencia telefónica y por correo electrónico para la instalación como se describe en `http://www.novell.com/products/linuxprofessional/support/conditions.html`. Para acceder a este servicio es necesario registrarse en el Portal de SUSE LINUX (`http://portal.suse.com`) mediante el código impreso en la carátula del CD.

Para que su sistema esté siempre seguro y al día, le recomendamos actualizarlo periódicamente por medio de YaST Online Update. SUSE le ofrece además un boletín electrónico gratuito que le informará regularmente acerca de temas de seguridad y le proporcionará trucos y consejos sobre SUSE LINUX. Si desea recibir este boletín, puede suscribirse con su dirección de correo electrónico en la página `http://www.novell.com/company/subscribe/`

El *Manual de administración* de SUSE LINUX le proporciona información general sobre el funcionamiento del sistema SUSE LINUX y le muestra los fundamentos de la administración de sistemas Linux: sistemas de archivos, kernel, proceso de arranque, la configuración del servidor web Apache, etc. El *Manual de administración* de SUSE LINUX está estructurado en cinco secciones principales:

Instalación Instalación y configuración del sistema con YaST, información detallada sobre variantes especiales de la instalación, LVM y RAID, actualización y reparación del sistema.

Sistema Particularidades del sistema SUSE LINUX, información detallada sobre el kernel, el concepto de arranque y el proceso de inicio, configuración del cargador de arranque y del sistema X Window, funcionamiento de la impresora y uso de dispositivos portátiles con Linux.

Servicios Integración en redes (heterogéneas), puesta en marcha de un servidor web Apache, sincronización de archivos y seguridad.

Administración Listas de control de acceso (ACLs) para sistemas de archivos e importantes herramientas de control del sistema.

Anexo Glosario y fuentes de información en torno a Linux.

Las versiones digitales de los manuales de SUSE LINUX se encuentran en el directorio `/usr/share/doc/manual/`.

Novedades en el manual de administración

A continuación le presentamos los cambios que se han producido en este manual con respecto a la versión anterior (SUSE LINUX 9.2):

- Se han revisado las secciones relativas a LVM y particionamiento (sección 3.6 en la página 100 y sección 2.7.5 en la página 73).
- El capítulo **??** en la página ?? se ha revisado y se ha añadido la descripción del módulo YaST así como una nueva sección sobre el uso de comodines (sección Selección del kernel de arranque mediante comodines en la página ??).
- El capítulo sobre los sistemas de archivos cuenta con una nueva sección dedicada a Reiser4: sección **??** en la página ??.
- La sección de redes del manual ha sido completamente revisada y reestructurada. Vea el capítulo **??** en la página ?? y siguientes.
- SuSEfirewall2 ha sido actualizado y se ha añadido una descripción del nuevo módulo de YaST (sección Configuración con YaST en la página ??).
- El capítulo **??** en la página ?? incluye la descripción de algunos programas nuevos.
- El glosario ha sido revisado y actualizado, ver también glosario **??** en la página ??.

Convenciones tipográficas

En este manual se utilizan las siguientes convenciones tipográficas:

- `/etc/passwd`: archivo o directorio.
- ⟨*Comodín*⟩: secuencia de caracteres que debe sustituirse por el valor real.
- `PATH`: variable de entorno con el nombre PATH.
- `ls`: comando.
- `--help`: opciones y parámetros.
- `user`: usuario.
- Alt: tecla que debe pulsarse.
- 'Editar': opciones del menú, botones.
- Process killed: mensajes del sistema.
- man man(1): referencia a páginas man.
- ► **x86, AMD64**
  Esta sección sólo es relevante para las arquitecturas especificadas. Las flechas marcan el comienzo y el final del bloque de texto. ◄

Agradecimientos

Desarrolladores de Linux de todo el mundo colaboran de forma desinteresada para impulsar la evolución de este sistema operativo. 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 a Pawar.

Asimismo, no queremos dejar de expresar nuestro más sincero agradecimiento a Linus Torvalds

Have a lot of fun!

Equipo SUSE

Índice general

Parte I

Instalación

La instalación con YaST

Este capítulo describe paso a paso el proceso de instalación de SUSE LINUX con el asistente del sistema YaST. Además le enseña a preparar el sistema para la instalación y le proporciona información complementaria sobre los distintos pasos de la configuración para facilitarle la toma de decisiones en lo que respecta a la configuración del sistema.

1.1. Arranque del sistema desde el medio de instalación

Introduzca el primer CD-ROM o el DVD de SUSE LINUX en el lector correspondiente. Después de reiniciar el ordenador, SUSE LINUX arranca desde el medio que se encuentra dentro del lector y se inicia el proceso de instalación.

1.1.1. Otras posibilidades de arranque

Además del inicio mediante el CD o DVD, dispone de otras posibilidades de arranque que pueden resultar de gran utilidad en caso de que surjan problemas al arrancar del CD o DVD. Estas opciones se describen en la tabla 1.1 en esta página.

Cuadro 1.1: *Opciones de arranque*

Opción de arranque	**Uso**
CD-ROM	Esta es la opción de arranque más sencilla. El único requisito es una unidad de CD-ROM disponible de manera local en el sistema y que esté soportada por Linux.
Disquete	El directorio `/boot/` del primer CD contiene las imágenes necesarias para crear disquetes de arranque. Consulte también el archivo `README` en el mismo directorio.
PXE o BOOTP	Esta opción ha de estar soportada por la BIOS o el firmware del sistema utilizado. Asimismo, en la red debe haber un servidor de arranque que puede ser también otro sistema SUSE LINUX.
Disco duro	Para poder arrancar SUSE LINUX desde el disco duro es necesario copiar en el disco duro el kernel (`linux`) y el sistema de instalación (`initrd`) que se encuentran en el directorio `/boot/loader` del primer CD. Además debe añadirse una entrada al cargador de arranque.

1.1.2. Posibles problemas al arrancar el sistema

En el momento de arrancar el sistema desde CD o DVD, pueden producirse problemas si el hardware del equipo es antiguo o no está soportado. Es posible que la unidad de CD-ROM no pueda leer la imagen de arranque (bootimage) del primer CD. En este caso utilice el CD 2 para arrancar el sistema. En este segundo CD se encuentra una imagen de arranque convencional de 2,88 MB que las unidades antiguas también pueden leer y que permite realizar la instalación desde la red.

Es posible que la secuencia de arranque del ordenador no esté configurada correctamente. La información para modificar la configuración de la BIOS (Basic Input Output System) se encuentra en la documentación de la placa base. A continuación se ofrecen unas instrucciones básicas para resolver este problema.

La BIOS es un elemento de software con el que se pueden arrancar la funcionalidad básica del ordenador. Los fabricantes de placas base proporcionan una BIOS a la medida del hardware. La configuración (setup) de la BIOS sólo puede activarse en un momento concreto: al arrancar el ordenador se realizan algunos diagnósticos del hardware, como por ejemplo de la memoria de trabajo. Al mismo tiempo se mostrará en la parte inferior de la pantalla o en la última línea mostrada, la tecla con la que puede iniciar la configuración de la BIOS. Suelen ser las teclas (Supr), (F1) o (Esc). La configuración de la BIOS se iniciará al pulsar la tecla correspondiente.

Importante

Tipo de teclado en la BIOS

Normalmente, la configuración de la BIOS ha de realizarse teniendo en cuenta una disposición de teclado para Estados Unidos.

Importante

Modifique la frecuencia de arranque de la siguiente forma. Si se trata de una AWARD BIOS, busque la entrada 'BIOS FEATURES SETUP'; otros fabricantes emplean entradas parecidas como por ejemplo 'ADVANCED CMOS SETUP'. Escoja la entrada correspondiente y confírmela pulsando (Intro).

Para modificar la secuencia de arranque es importante el punto que se encuentra en el orden de arranque de la unidad. La configuración por defecto a menudo es C, A o bien A, C. En el primer caso, el ordenador intenta arrancar el sistema primero desde el disco duro (C) y después desde la disquetera (A). Escoja 'Boot Sequence' y pulse las teclas (PgUp) o (PgDown), hasta que se muestre la secuencia `A, CDROM, C`.

Abandone la configuración pulsando Esc. Para grabar los cambios, escoja 'SAVE & EXIT SETUP' o pulse F10. Confirme la configuración con Y.

Si tiene una unidad CD ROM SCSI, para invocar la BIOS de, por ejemplo, una controladora Adaptec, deberá utilizar Ctrl-A. Escoja la opción 'Disk Utilities'. El sistema mostrará el hardware conectado. Anote el ID SCSI de su CD ROM. Abandone el menú con Esc para abrir a continuación 'Configure Adapter Settings'. En 'Additional Options' verá 'Boot Device Options'. Escoja este menú y pulse Intro. Ahora introduzca el ID de la unidad de CD ROM que anotó y pulse Intro. Al pulsar dos veces en Esc volverá a la pantalla de inicio de la BIOS SCSI, que podrá abandonar con 'Yes', tras lo que el ordenador volverá a arrancar.

1.2. La pantalla de bienvenida

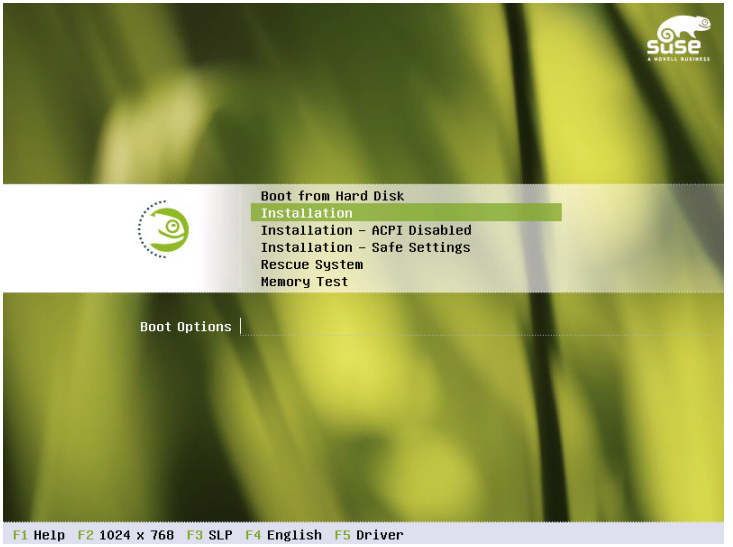

Figura 1.1: *La pantalla de bienvenida*

La pantalla de inicio muestra varias posibilidades para el desarrollo posterior del proceso de instalación. En la parte superior se encuentra la opción 'Boot from Harddisk', que arranca el sistema ya instalado. Debido a que una vez realizada

la instalación a menudo se introduce el CD para instalar otros componentes de software, esta opción está preseleccionada. Emplee las teclas de cursor (flechas) para seleccionar una de las opciones de instalación. Las diferentes alternativas son:

Installation La instalación normal en la que se activan todas las funciones actuales del hardware.

Installation—ACPI Disabled Cuando la instalación normal no funciona, es posible que el ordenador no sea capaz de trabajar correctamente con el soporte ACPI (Advanced Configuration and Power Interface). En tal caso es aconsejable realizar la instalación sin soporte ACPI.

Installation—Safe Settings Desactiva la función DMA (para la unidad de CD-ROM) y la gestión de energía. Los expertos también pueden modificar o introducir parámetros del kernel en la línea de entrada.

Como se indica en la barra de teclas de función, que está situada en el borde inferior de la ventana de instalación, puede utilizar las teclas F para configurar distintas opciones para la instalación:

(F1) Se muestra una ayuda contextual sobre el elemento activo en ese momento en la pantalla de bienvenida.

(F2) Puede seleccionar distintos modos gráficos para la instalación. Si surgen problemas en la instalación en modo gráfico, esta opción le permite también seleccionar el modo texto.

(F3) El sistema se instala normalmente desde el medio de instalación introducido. No obstante, aquí puede seleccionar otras fuentes de instalación como FTP y NFS. Cabe destacar SLP (Service Location Protocol). En el caso de una instalación en una red con un servidor SLP, esta opción permite seleccionar una de las fuentes de instalación disponibles en el servidor antes de que dé comienzo la auténtica instalación. Puede obtener información adicional sobre SLP en el capítulo **??** en la página ??.

(F4) Aquí puede seleccionar el idioma para la instalación.

(F5) Si dispone de un disquete de actualización de controladores para SUSE LINUX, esta opción le permite utilizarlo. En el transcurso de la instalación se le pedirá que introduzca el medio de actualización.

Al cabo de unos segundos, SUSE LINUX carga un sistema Linux mínimo que controlará el resto del proceso de instalación. Si ha cambiado el modo de salida en pantalla a 'Native' o 'Verbose', verá a continuación numerosos mensajes y avisos de copyright. Al final del proceso de carga se inicia el programa de instalación YaST, y unos segundos después aparece la interfaz gráfica de usuario.

Ahora empieza la verdadera instalación de SUSE LINUX. Todas las pantallas de YaST siguen un esquema uniforme. Se puede acceder con el ratón y el teclado a todos los botones, casillas de texto y listas de selección de las pantallas de YaST. Si el cursor no se mueve, significa que el ratón no ha sido detectado automáticamente. Emplee en este caso el teclado. La forma de navegar mediante el teclado es similar a la descrita en la sección 2.9.1 en la página 83

1.3. Selección del idioma

Es posible seleccionar el idioma deseado para SUSE LINUX y YaST. El idioma elegido se aplica también a la configuración del teclado y YaST define además una zona horaria estándar que es la más apropiada para su configuración de idioma. Estas opciones pueden modificarse posteriormente junto con la selección de idiomas secundarios que desee instalar en el sistema. Si el ratón todavía no funciona, utilice las flechas del teclado hasta llegar al idioma deseado, a continuación pulse (Tab) hasta que el botón 'Siguiente' esté activado y finalmente pulse la tecla (Intro).

1.4. Modo de instalación

El usuario puede decidir si quiere realizar una 'Nueva Instalación' o 'Actualizar un sistema existente'. Evidentemente sólo puede realizar una actualización si ya tiene SUSE LINUX instalado. Este sistema ya instalado se puede arrancar con la opción 'Arrancar el sistema instalado'. Si en algún caso el sistema SUSE LINUX dejara de arrancar (p.ej. porque se ha borrado accidentalmente una parte importante del sistema), puede utilizar la opción 'Reparar el sistema instalado' para intentar que el sistema pueda arrancarse de nuevo. Si hasta ahora no ha instalado ningún sistema SUSE LINUX, sólo puede realizar una instalación nueva (figura 1.3 en la página 10).

En este capítulo nos limitaremos a describir una instalación nueva. Puede obtener más información en la sección 2.2.4 en la página 51. La descripción de las posibilidades del arreglo de sistema se encuentran en el capítulo **??** en la página ??.

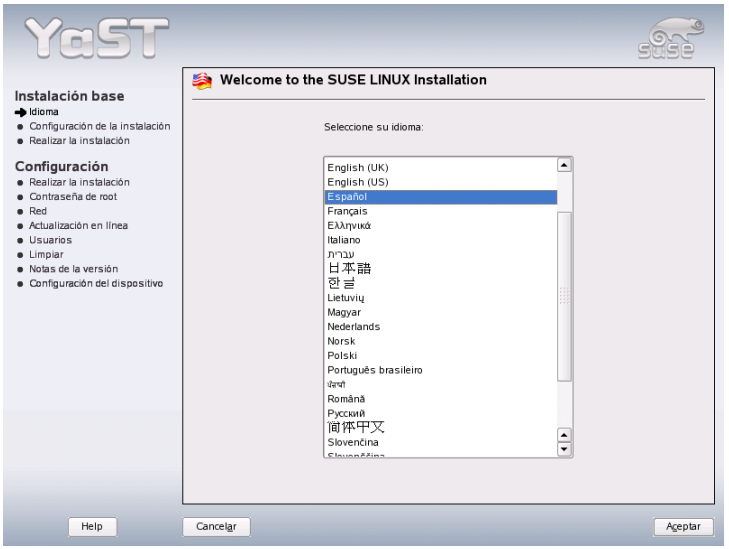

Figura 1.2: *Selección del idioma*

1.5. Propuesta para la instalación

Después de la detección del hardware, aparecerá el diálogo de propuestas (ver figura 1.4 en la página 11) con información sobre el hardware detectado y las propuestas de instalación y de particiones. Si pulsa sobre una de las opciones y después la configura, al acabar siempre volverá a aparecer con los nuevos valores en el mismo diálogo de propuestas. A continuación se describen las distintas opciones de configuración para la instalación.

1.5.1. Modo de instalación

En este punto se puede cambiar el modo de instalación. Las posibilidades son las mismas la sección 1.4 en la página anterior.

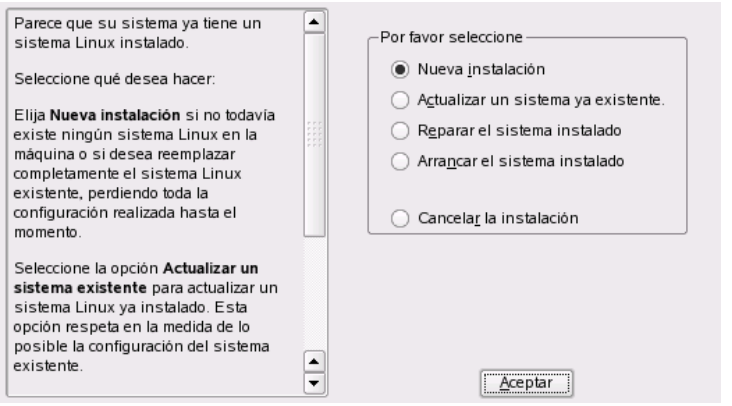

Figura 1.3: *Selección del modo de instalación*

1.5.2. Configuración del teclado

Seleccione en este diálogo la distribución del teclado deseada. Generalmente coincide con el idioma seleccionado. Compruebe la configuración pulsando algunas teclas, sobre todo `y/z` y los caracteres acentuados. Si no aparecen los caracteres esperados, es porque la distribución del teclado aún no es la correcta. Con 'Siguiente' puede volver a las propuestas.

1.5.3. Ratón

En caso de que YaST no haya detectado automáticamente el ratón, muévase con la tecla (Tab) hasta que esté activado 'Cambiar'. Pulse entonces (Espacio) y después las teclas de dirección hasta llegar al punto 'Ratón'. Pulsando (Intro) aparece el diálogo de la figura 1.5 en la página 12 para la selección del tipo de ratón.

Utilice las teclas ↑ y ↓ para seleccionar el ratón. Si conserva la documentación del ratón, encontrará allí una descripción del tipo de ratón. Con la combinación de teclas (Alt)-(T) puede seleccionar el ratón temporalmente para probarlo. Si el ratón no reacciona como se espera, seleccione un nuevo tipo con el teclado y compruébelo. Pulse (Tab) e (Intro) para hacer la selección permanente.

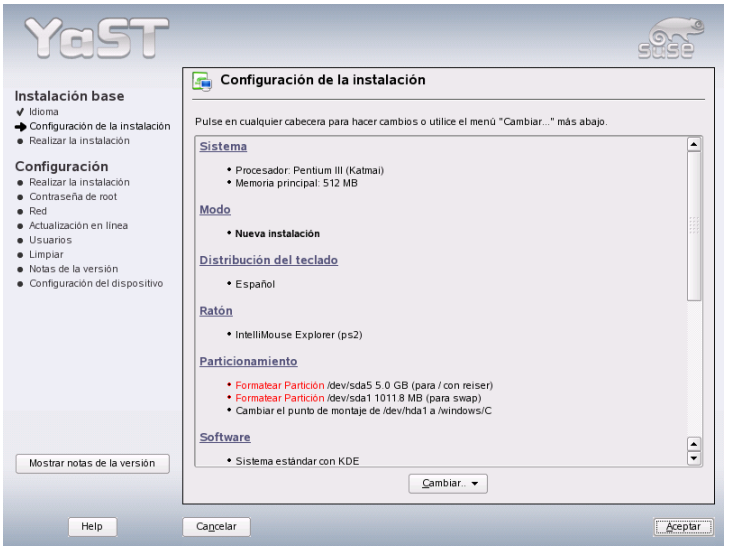

Figura 1.4: *Ventana de diálogo de propuestas*

1.5.4. Particionar

En la mayoría de los casos basta con la propuesta de particiones realizada por YaST y no se requiere ninguna modificación. Pero si quiere efectuar una distribución especial del disco duro, también puede hacerlo. A continuación le indicamos cómo.

Tipos de particiones

Cada disco duro contiene una tabla de particiones con espacio para cuatro entradas. Una entrada puede corresponder a una partición primaria o a una extendida. No obstante, sólo es posible disponer de una partición extendida..

La estructura de las particiones primarias es relativamente simple, pues se trata de una zona continua de cilindros (áreas físicas del disco) que está asignada a un sistema operativo. Con particiones primarias, solamente se puede establecer un máximo de cuatro; no caben más en la tabla de particiones. De aquí parte el concepto de la partición extendida, la que también se representa como una zona continua de cilindros. Sin embargo, es posible dividir la partición extendida en

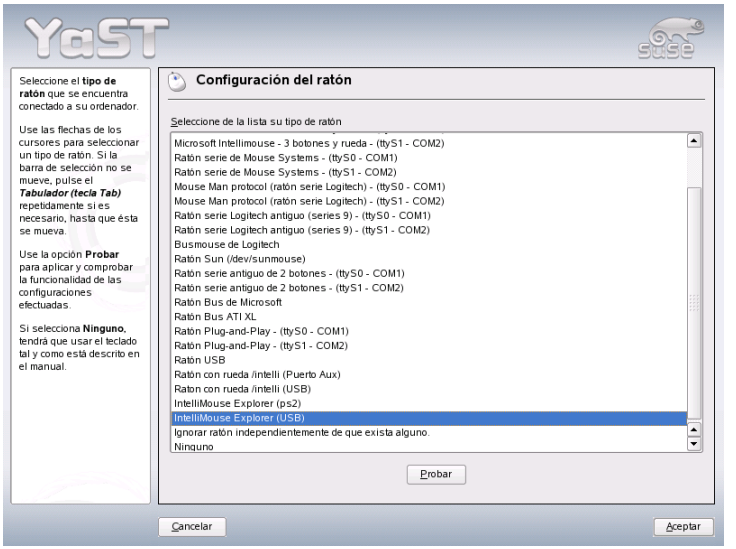

Figura 1.5: *Selección del ratón*

particiones lógicas que no necesitan una entrada en la tabla de particiones. Se puede decir que se trata de una especie de contenedor para las particiones lógicas.

Si se necesitan más de cuatro particiones es necesario definir la cuarta como partición extendida y asignar a ella todos los cilindros libres. En ésta se pueden generar entonces *casi* tantas particiones como se desee (el máximo se sitúa en 15 para discos SCSI, SATA y Firewire y 63 para unidades E(IDE). Para instalar SUSE LINUX son apropiadas ambas clases de particiones, tanto las primarias como las lógicas.

Sugerencia

Discos duros con etiqueta GPT

En aquellas arquitecturas que utilicen la etiqueta de disco GPT, el número de particiones primarias no está restringido. Por tanto, las particiones lógicas no existen en este caso.

Sugerencia

Requerimientos de espacio en disco

Si deja que YaST efectúe las particiones del disco duro, no deberá preocuparse de las necesidades de espacio en disco y del reparto del disco. En caso de que efectúe las particiones Vd. mismo, se indican a continuación algunas notas sobre los requisitos de espacio de los distintos tipos de sistemas.

Sistema mínimo: 500 MB Este sistema no tiene interfaz gráfica (X11), es decir, sólo puede trabajar en consola. Además sólo permite la instalación del software más elemental.

Sistema mínimo con interfaz gráfica: 700 MB
Aquí puede al menos instalar X11 y algunas aplicaciones.

Sistema estándar: 2,5 GB Aquí pueden instalarse los modernos escritorios KDE o GNOME así como aplicaciones "grandes" como por ejemplo OpenOffice, Netscape y Mozilla.

Aunque el esquema de particiones depende en gran medida del espacio disponible, existen algunas líneas generales que cabe considerar:

Hasta 4 GB: Una partición de intercambio (swap) y una partición root (`/`). La partición root incluye los directorios para los que se utilizan particiones propias en el caso de discos duros de grandes dimensiones.

Propuesta a partir de 4 GB: Swap, root (1 GB) y, en caso necesario, una partición respectivamente para `/usr` (mínimo 4 GB), `/opt` ((mínimo 4 GB) y `/var` (1 GB). El resto del espacio puede asignarse a `/home`.

Dependiendo del hardware del ordenador, puede ser necesario configurar al principio del disco duro una partición de arranque (`/boot`) para los archivos de inicio y el kernel de Linux. Es recomendable que el tamaño de esta partición sea al menos de 8 MB o comprenda un cilindro. Puede aplicar la siguiente regla con carácter orientativo: si YaST sugiere una partición de arranque, también debe configurar una al definir las particiones manualmente. En caso de duda lo más seguro es crear una partición de arranque.

Se debe tener en cuenta que algunos programas – generalmente comerciales – instalan sus datos en `/opt`, así que es conveniente generar una partición propia para `/opt` o bien hacer la partición root más grande. KDE y GNOME se encuentran igualmente en el directorio `/opt`.

Particionar con YaST

Si ha seleccionado la partición en la ventana de diálogo de propuestas, aparecerá el diálogo de particiones de YaST con la configuración actual. Puede aceptar, cambiar o eliminar las opciones de configuración en caso de que quiera realizar una nueva distribución del espacio.

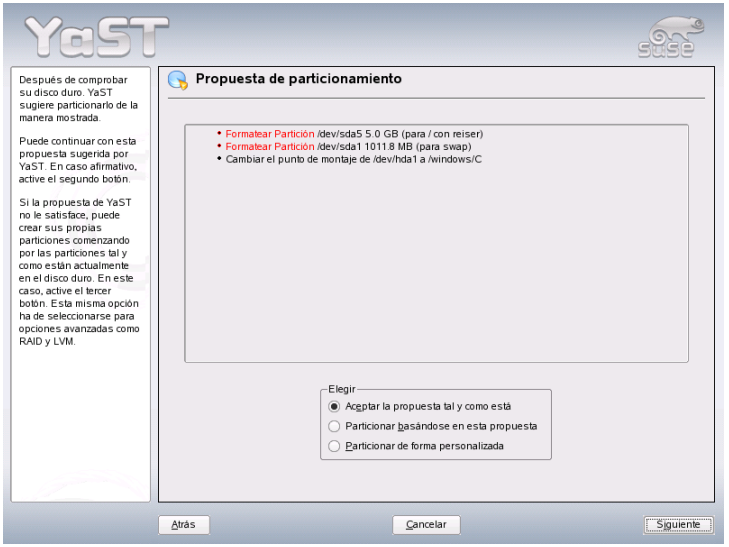

Figura 1.6: *Editar propuesta de particiones*

Al seleccionar 'Aceptar la propuesta tal y como está', no se efectuará ninguna modificación y el diálogo de propuesta se quedará como está. Al seleccionar 'Particionar basándose en esta propuesta', aparecerá directamente el diálogo para expertos que permite definir opciones de configuración muy detalladas (véase la sección 2.7.5 en la página 73). La propuesta de partición de YaST también aparece y se puede modificar.

Al escoger 'Particionar de forma personalizada', aparecerá un diálogo en el que se puede seleccionar el disco duro (figura 1.7 en la página siguiente). Aquí verá una lista de todos los discos duros disponibles en el sistema. Escoja aquel en el que quiera instalar SUSE LINUX

Después de seleccionar un disco duro puede especificar si se debe utilizar 'Todo el disco' o si sólo se debe instalar en una de las particiones (en caso de que estén

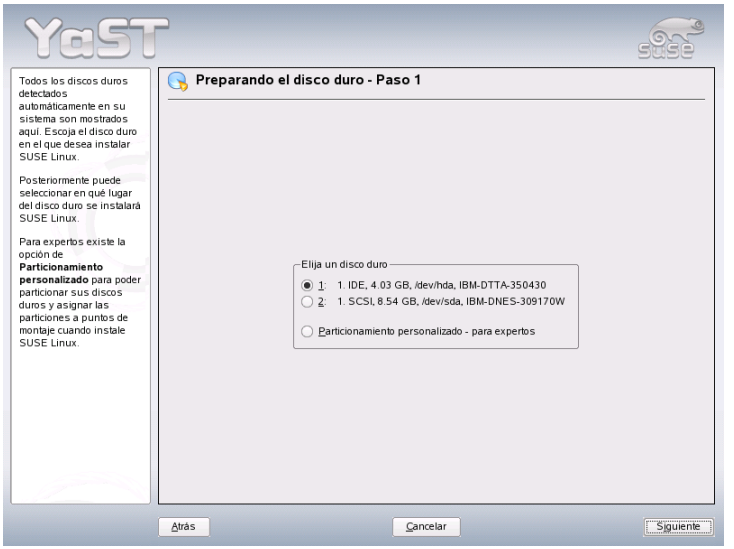

Figura 1.7: *Selección del disco duro*

disponibles). Si el disco duro seleccionado tiene un sistema operativo Windows, se le preguntará si quiere eliminar o reducir Windows. En caso afirmativo, lea la sección Adaptación de una partición Windows en la página siguiente. Si no es así, pase al diálogo de expertos en el que puede configurar las particiones que desee (véase la sección 2.7.5 en la página 73).

Aviso

Utilización de todo el disco duro para la instalación

Al seleccionar 'Todo el disco' se perderán todos los datos de este disco duro.

Aviso

A continuación YaST comprueba que el espacio en el disco duro sea suficiente para el software seleccionado. Si no lo es, la selección de software se modificará de forma automática y la indicación correspondiente aparecerá en el diálogo de propuestas. En caso de que sí haya suficiente espacio de memoria, YaST guardará la configuración definida y distribuirá el disco duro según el espacio asignado.

Adaptación de una partición Windows

Si al particionar un disco duro ha seleccionado bien una partición FAT de Windows o bien una partición NTFS de Windows como destino de instalación, YaST le ofrece la posibilidad de eliminar o reducir dicha partición. De este modo, también se puede instalar SUSE LINUX aunque no haya suficiente espacio libre en el disco duro. Esto es recomendable cuando sólo existe una partición con Windows en el disco duro, lo que suele ser habitual en algunos de los ordenadores en los que ya hay un sistema operativo instalado. Si YaST detecta que el espacio disponible en el disco duro seleccionado es demasiado pequeño para la instalación y que dicho problema se puede solucionar eliminando o reduciendo una partición de Windows, aparecerá una ventana de diálogo en la que puede seleccionar la opción deseada.

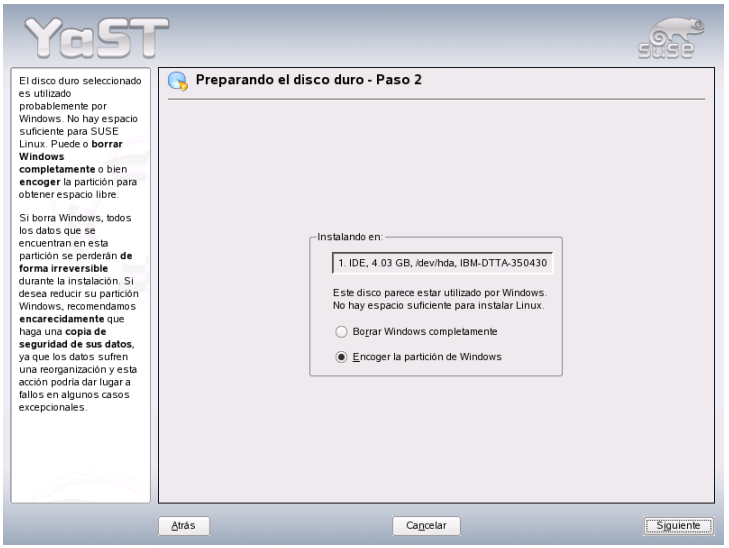

Figura 1.8: *Posibles opciones con particiones Windows.*

Si selecciona 'Borrar Windows por completo', se eliminará la partición Windows y el espacio que ha dejado libre se utilizará para instalar SUSE LINUX.

Aviso

Eliminar Windows

En caso de que decida eliminar Windows debe tener en cuenta que perderá todos sus datos durante la instalación de Linux de forma irrecuperable.

Aviso

Si decide reducir la partición Windows, primero debe cancelar la instalación y arrancar Windows para efectuar allí algunos pasos preliminares. Esto no es totalmente necesario para particiones FAT, pero acelera y vuelve más seguro el proceso de reducción de la partición Windows FAT. Estos pasos son imprescindibles para particiones NTFS.

Sistema de archivos FAT Para ello ejecute en Windows el programa scandisk para asegurarse de que el sistema de archivos FAT se encuentra libre de errores de encadenamiento. Después mueva los archivos con defrag al principio de la partición, lo que acelera el posterior proceso de reducción en Linux.

Si ha optimizado la configuración de la memoria virtual de Windows de tal forma que se use un archivo swap contiguo con un límite superior e inferior idéntico para el tamaño, es necesario llevar a cabo otro preparativo. En este caso, puede que en el proceso de reducción los archivos swap se rompan y que se pierda toda la partición Windows. Además, en este mismo proceso hay que mover los archivos swap, lo que hace alarga aún más dicho proceso de reducción. Por lo tanto, debe anular dicha optimización y volver a realizar la reducción.

Sistema de archivos NTFS Ejecute aquí también scandisk y después defrag para mover los archivos al principio de la partición. Al contrario que en el sistema de archivos FAT, en NTFS es imprescindible realizar esta acción para que la partición pueda ser reducida.

Importante

Reducir la partición swap en Windows

Si su sistema trabaja con un archivo de intercambio (swap) permanente en un sistema de archivos NTFS, es posible que este archivo se encuentre al final del disco duro y que se quede inamovible aunque se utilice defrag. Una consecuencia de ello podría ser que la partición no pudiese reducirse lo suficiente. Para resolver el problema, desactive en Windows temporalmente la partición de intercambio (memoria virtual). Puede volver a activarla después de haber reducido la partición.

Importante

Una vez realizados estos preparativos, seleccione en el diálogo de partición la opción 'Redimensionar la partición Windows'. Después de una corta comprobación, YaST abre una nueva ventana de diálogo con una propuesta razonable para reducir la partición de Windows.

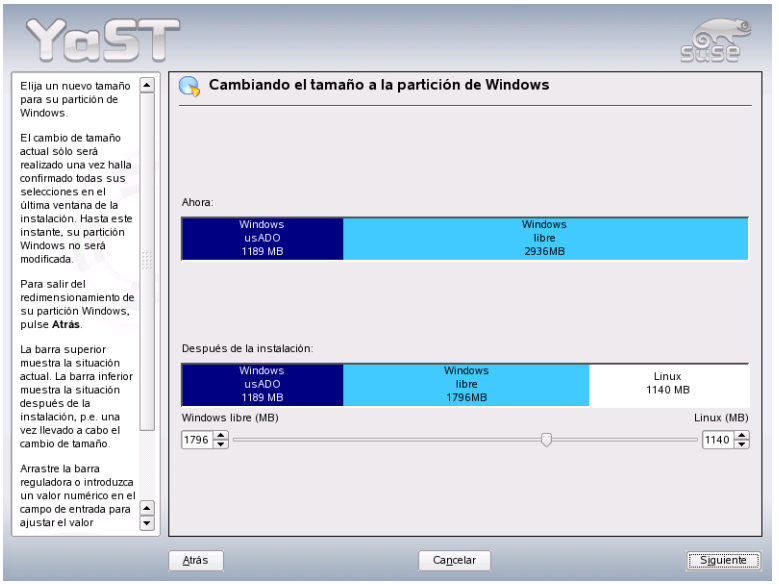

Figura 1.9: *Adaptación de una partición Windows.*

YaST visualiza en el primer diagrama de barras la cantidad de espacio ocupado por Windows en la actualidad y también el espacio libre del disco duro. El segundo diagrama le hace una sugerencia sobre la nueva división del disco duro (figura 1.9 en la página anterior). Puede aceptar la sugerencia o cambiar los límites mediante la barra de desplazamiento.

Si abandona este diálogo con 'Siguiente', se grabarán las configuraciones actuales y volverá al diálogo anterior. La reducción no se efectuará inmediatamente, sino más tarde, justo antes de que se formatee el disco duro.

Importante

Windows con sistema de archivos NTFS

Las versiones NT, 2000 y XP de Windows utilizan como estándar el sistema de archivos NTFS. Actualmente Linux sólo puede leer un sistema de archivos NTFS, pero no escribirlo como es el caso en los sistemas de archivos FAT. Por eso desde Linux sólo puede leer los datos de NTFS pero no modificar y grabarlos. Para tener también acceso de escritura en los archivos residentes en Windows, instale éste nuevamente sobre un sistema de archivos FAT32.

Importante

1.5.5. Software

SUSE LINUX incluye una gran cantidad de software que se instala según el perfil del usuario. Seleccionar por separado los paquetes de software del gran conjunto disponible sería muy tedioso. Por este motivo, SUSE LINUX ofrece varios subconjuntos preconfigurados. De acuerdo al espacio de disco disponible, YaST selecciona automáticamente uno de estos subconjuntos y muestra esta propuesta.

Mínima (recomendada sólo para aplicaciones especiales)
Sólo se instala el sistema operativo con diferentes servicios. No hay entorno gráfico y el control del ordenador se realiza por medio de consolas de texto. Este tipo de sistema es ideal para aplicaciones de servidor que requieren poca o ninguna interacción con el usuario.

Sistema gráfico mínimo (sin KDE o GNOME)
Si le falta espacio de disco o no desea los escritorios KDE o GNOME, instale este conjunto de software. El sistema dispondrá de X Window y un entorno gráfico básico. Sin embargo, pueden utilizarse todos los programas que

cuentan con una interfaz gráfica propia.No se instala ningún programa ofimático.

Sistema estándar con GNOME y paquete ofimático
: Este es el sistema estándar más grande disponible. Contiene el escritorio GNOME con la mayoría de sus programas y los paquetes ofimáticos.

Sistema estándar con KDE y paquete ofimático
: Este es el sistema estándar más grande disponible. Contiene el escritorio KDE con la mayoría de sus programas y los paquetes ofimáticos.

Al pulsar 'Software' en el apartado de propuestas puede seleccionar uno de los sistemas básicos. Además puede iniciar el módulo de selección de software (es decir, el administrador de paquetes), pulsando en 'Selección detallada' para modificar individualmente la selección de software instalada.(ver figura 1.10 en esta página).

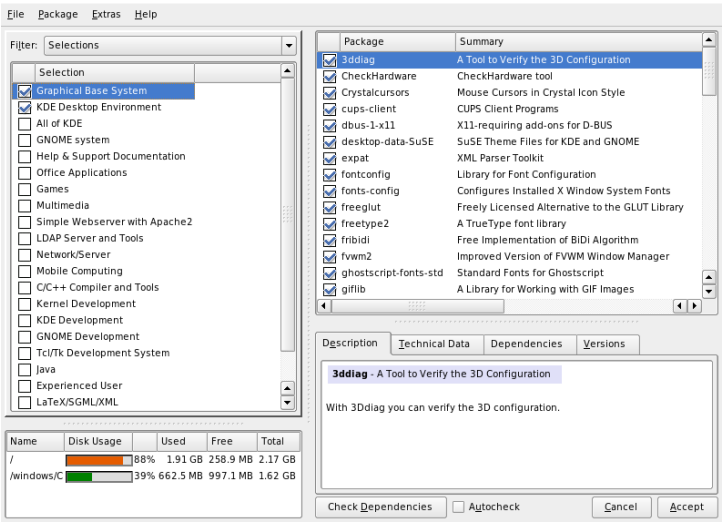

Figura 1.10: *YaST: instalar y eliminar software (administrador de paquetes)*

Modificar conjunto de software predefinido

Al instalar el sistema estándar normalmente no hace falta modificar la selección de paquetes, ya que este sistema satisface todos los requisitos del usuario medio.

Sin embargo existe la posibilidad de realizar intervenciones manuales mediante el gestor de paquetes. Este gestor permite seleccionar algunos de los muchos paquetes en SUSE LINUX utilizando filtros.

La ventana de selección de filtros se encuentra en la parte superior izquierda. Está activado al iniciar el filtro de selecciones. Las selecciones agrupan los programas según su utilidad, p.ej. Multimedia u Ofimática. Por debajo del área de selección de filtros se puede ver aquellos que ya fueron seleccionados y que pertenecen al sistema predefinido. Al pulsar en la casilla correspondiente se activa o desactiva una determinada selección.

En la ventana de la derecha puede ver una lista de los paquetes que se incluyen en esa selección. Todos los paquetes tienen un estado actual. En el punto de la instalación en el que se encuentra, los estados más interesantes son instalar y no instalar, o sea una marca a la izquierda del nombre del paquete o una casilla vacía. Aquí puede escoger o deseleccionar paquetes individuales. Para ello pulse en el símbolo de la izquierda hasta que se muestre el estado deseado (instalar o no instalar). Pulsando con el botón derecho sobre la línea del paquete, se abre un menú desplegable que muestra los diferentes estados. Los estados restantes se explican en las instrucciones detalladas sobre este módulo en la sección 2.2.1 en la página 40.

Otros filtros

Si abre el menú de selección de filtros, verá una selección de filtros adicionales que le ayudarán a ordenar los paquetes. La opción más interesante es la selección según 'Grupos de paquetes'. Con este filtro verá los paquetes de programa en la parte izquierda ordenados por temas en una estructura de árbol. Cuanto más se adentre en la estructura de árbol, más exacta es la selección y más pequeña es la cantidad de paquetes que aparecen en la lista de paquetes de la derecha.

'Buscar' sirve para buscar un paquete determinado; más información en la sección 2.2.1 en la página 40.

Dependencias de paquetes y conflictos

No es posible instalar cualquier combinación de software. Los paquetes instalados deben ser compatibles entre sí. Si no se respeta esta regla, puede haber contradicciones que pongan en peligro el buen funcionamiento del sistema instalado. Por eso pueden aparecer advertencias sobre conflictos o dependencias no resueltas al seleccionar paquetes en esta ventana de diálogo. Si no entiende el significado de estas advertencias, diríjase a la sección 2.2.1 en la página 40. Allí encontrará

información detallada sobre el manejo del gestor de paquetes y explicaciones sobre la organización del software en Linux.

Aviso

La selección estándar que se le propone en la instalación es la más aconsejable tanto para los principiantes como para los usuarios avanzados. Por lo general no es necesario realizar aquí ninguna modificación. Si decide seleccionar o no seleccionar determinados paquetes, asegúrese de que sabe lo que está haciendo. Al desinstalar paquetes, tenga en cuenta los mensajes de aviso y no escoja ningún paquete que pertenezca al sistema básico de Linux.

Aviso

Terminar selección de software

Cuando la selección de software haya terminado y ya no existan dependencias sin resolver o conflictos entre paquetes, pulse 'Aceptar' para salir del programa. Durante la instalación, los cambios se registran y se aplican posteriormente cuando se inicia la verdadera instalación.

1.5.6. El inicio del sistema (instalación del cargador de arranque)

YaST determina correctamente el modo de arranque durante la instalación por lo que, en circunstancias normales, puede adoptar estas configuraciones sin necesidad de modificarlas. No obstante, si necesita cambiar la configuración predeterminada debido a requisitos especiales del sistema, también podrá hacerlo.

Puede por ejemplo cambiar la configuración para que sea necesario introducir un disquete de arranque especial a la hora de arrancar SUSE LINUX. Este puede ser el caso si normalmente trabaja con otro sistema operativo cuyo mecanismo de arranque no se deba modificar. Por lo general, no es necesario porque YaST configura el gestor de arranque de tal forma que Vd. selecciona cuál de los dos sistemas operativos debe arrancar. Más adelante, si lo desea, también podrá cambiar la ubicación del gestor de arranque de SUSE LINUX dentro del disco duro.

Si quiere cambiar la propuesta de YaST, seleccione la opción 'Arranque'. Aparecerá un diálogo que permite acceder al mecanismo de arranque. Para más información lea la sección **??** en la página ??. Se recomienda que sólo los expertos cambien el modo de arranque.

1.5.7. Configuración de la zona horaria

En este diálogo (figura 1.11 en esta página), en el campo 'Reloj de hardware configurado para', puede elegir entre las opciones 'Hora local' y 'GMT'. Su selección depende de la configuración del reloj en la BIOS del ordenador. Si está configurado con el valor `GMT`, SUSE LINUX se encarga de cambiar automáticamente entre horario de verano y de invierno.

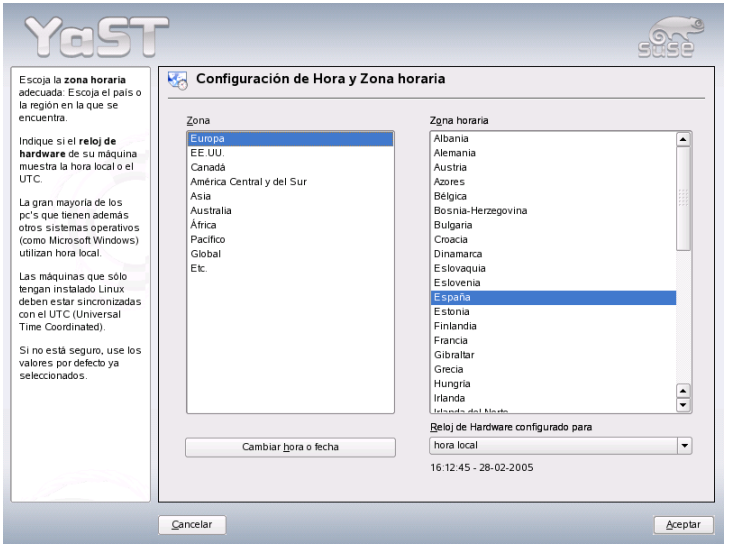

Figura 1.11: *Selección de la zona horaria.*

1.5.8. Idioma

El idioma ya se seleccionó al principio de la instalación (ver sección 1.3 en la página 8). Sin embargo, aquí puede modificarlo posteriormente además de seleccionar idiomas adicionales que deban instalarse en el sistema. En la parte superior del diálogo puede definir el idioma principal que se activará tras la instalación. Si lo desea, dispone de dos opciones para ajustar la configuración del teclado y la zona horaria en función del idioma principal. También tiene la posibilidad de

configurar el idioma para el usuario `root` pulsando el botón 'Detalles'. El menú desplegable ofrece tres opciones:

ctype only El archivo `/etc/sysconfig/language` albergará el valor de la variable `LC_CTYPE`. Esto define la activación de las funciones que dependen del idioma seleccionado.

yes El usuario `root` tiene exactamente la misma configuración de idioma que el usuario local.

no La configuración de idioma del usuario `root` será independiente de la selección de idioma general.

Algunos administradores de sistemas no quieren que el entorno de `root` se ejecute con soporte multilenguaje UTF-8. Si ese es su caso, desactive la opción 'Utilizar codificación UTF-8'.

En la lista de la parte inferior de este diálogo puede seleccionar idiomas adicionales para instalar en el sistema. YaST lee los idiomas seleccionados en la lista y comprueba si existen paquetes de idioma específicos para alguno de los paquetes de la selección actual de software. En caso afirmativo se instalan esos paquetes.

Pulse 'Aceptar' para finalizar la configuración o 'Cancelar' para deshacer los cambios.

1.5.9. Realizar la instalación

Al pulsar 'Siguiente' acepta la propuesta con todos los cambios realizados por Vd. y accede al diálogo de confirmación. Si elige 'Sí, instalar' la instalación se inicia con las opciones seleccionadas. Dependiendo de la capacidad de la CPU y la selección de software, la instalación dura generalmente entre 15 y 30 minutos. Después de la instalación de paquetes, YaST inicia el sistema instalado antes de continuar con la configuración del hardware y los servicios.

1.6. Completar la instalación

Una vez que el sistema y el software seleccionado han sido instalados, deberá especificar una contraseña para el administrador del sistema (usuario `root`). A continuación tendrá la oportunidad de configurar el acceso a Internet y la conexión de red. De esta forma podrá instalar actualizaciones de software para SUSE

LINUX durante la instalación. También puede configurar un servidor de autenticación para la administración centralizada de usuarios en la red local. Finalmente, podrá configurar los dispositivos de hardware conectados.

1.6.1. Contraseña de root

Root es el nombre del superusuario o administrador del sistema que tiene todos los permisos de los que carece un usuario normal. Puede cambiar el sistema, instalar programas nuevos para todos o configurar hardware nuevo. `root` puede ayudar cuando alguien ha olvidado su contraseña o cuando un programa ha dejado de funcionar. Generalmente el uso de la cuenta `root` debería limitarse para realizar tareas administrativas, trabajos de mantenimiento y arreglos. En el quehacer cotidiano es arriesgado trabajar como `root`, ya que root podría por ejemplo borrar por descuido todos los archivos de forma irrecuperable.

Para definir la contraseña de `root` tiene que seguir el mismo proceso que para definir la contraseña de un login normal. Hay que introducir la contraseña dos veces para su comprobación (figura 1.12 en la página siguiente). Es muy importante recordar bien la contraseña de `root` ya que posteriormente no hay ninguna posibilidad de consultarla.

Aviso

El usuario root

El usuario `root` tiene todos los permisos y puede realizar todos los cambios en el sistema. Si quiere llevar a cabo tales tareas necesita la contraseña especialmente definida para `root`. Sin esta contraseña no es posible realizar tareas administrativas.

Aviso

1.6.2. Configuración de red

En el siguiente paso tiene la oportunidad de conectar su sistema al resto del mundo. Puede configurar la tarjeta de red, RDSI, módem y DSL. Si el sistema está equipado con este tipo de hardware, aproveche esta ocasión. En ejecuciones posteriores de YaST se pueden descargar actualizaciones de Internet para SUSE LINUX que se tendrán en cuenta durante la instalación.

[SEGUIR AQUI]Si quiere configurar el hardware de red en este punto, busque las secciones correspondientes en la sección **??** en la página ??. Si no es el caso,

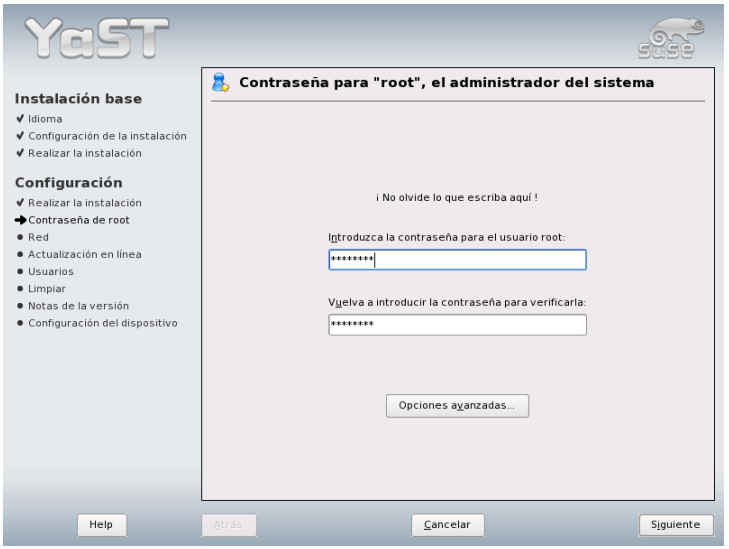

Figura 1.12: *Setting the root Password*

seleccione la opción 'Omitir configuración de red' y pulse en 'Siguiente'. Siempre puede configurar posteriormente el hardware de red en el sistema instalado.

1.6.3. Configuración del cortafuegos

En cuanto conecte el sistema a una red, se iniciará automáticamente un cortafuegos en la interfaz configurada. La configuración del cortafuegos se muestra en el diálogo de configuración de la red. Cada vez que se modifique la configuración de la interfaz o el servicio, se actualizará automáticamente la propuesta de configuración del cortafuegos. Si desea personalizar la configuración predefinida pulse en 'Cambiar' → 'Cortafuegos'. En el diálogo que se abre a continuación puede seleccionar si el cortafuegos debe iniciarse o no. Si no desea que el cortafuegos sea activado, marque la opción correspondiente y salga del diálogo. Si, por el contrario, desea iniciar el cortafuegos y continuar su configuración, pulse 'Siguiente' para acceder a una secuencia de diálogos similar a la descrita en la sección Configuración con YaST en la página ??.

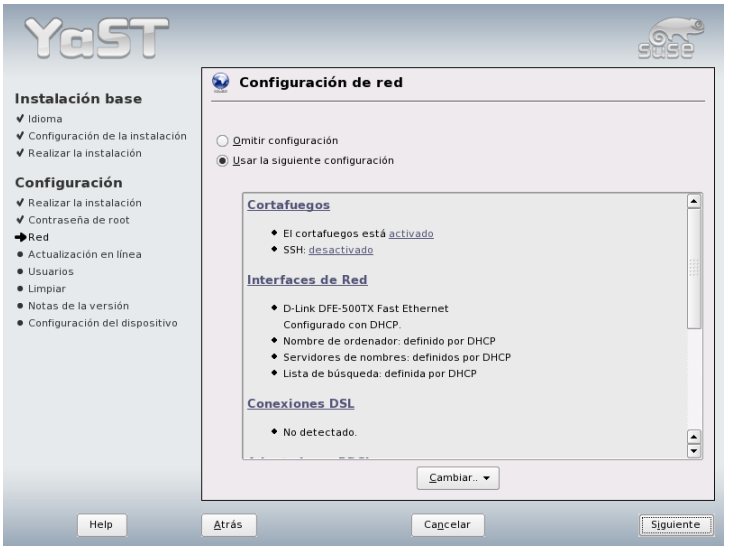

Figura 1.13: *Configuración de los dispositivos de red*

1.6.4. Comprobar la conexión a Internet

Si ha configurado una conexión a Internet, ahora puede comprobar si funciona correctamente. Para ello, YaST establece una conexión con el servidor de SUSE y comprueba al mismo tiempo si hay actualizaciones disponibles para SUSE LINUX. Si la conexión funciona adecuadamente, puede proceder a descargar estas actualizaciones en el paso siguiente. Además se obtienen del servidor las últimas notas de versión y al final de la descarga se muestran en pantalla.

Si no quiere comprobar la conexión a Internet en este punto, seleccione 'Saltar test' y pulse en 'Siguiente'. Tampoco se realizará la actualización de los productos ni obtendrá las últimas notas de versión.

1.6.5. Descargar actualizaciones de software

Si en el paso anterior YaST se ha conectado con éxito a Internet, se le ofrecerá la posibilidad de realizar una actualización en línea con YaST (YaST Online Update).

Figura 1.14: *Comprobar la conexión a Internet*

En caso de que en el servidor SUSE se encuentren parches para errores o problemas de seguridad conocidos, podrá instalarlos y aplicarlos.

Importante

Descargar actualizaciones de software

La duración del proceso de actualización depende de la capacidad de la conexión a Internet y del tamaño de los paquetes de actualización.

Importante

Si quiere ejecutar una actualización de software inmediatamente, seleccione 'Sí, realizar actualización en línea' y confirme con 'Aceptar'. A continuación aparecerá el diálogo de actualización en línea de YaST donde puede ver los parches disponibles, seleccionar los que desee y aplicarlos. Consulte a este respecto la sección 2.2.3 en la página 49. Por supuesto, también puede realizar esta actualización más tarde. Para ello, seleccione 'No, saltarse la actualización' y pulse 'Aceptar'.

1.6.6. Autenticación de usuarios

Una vez configurada una conexión a Internet durante la instalación, tiene cuatro posibilidades para administrar los usuarios del sistema instalado.

Administración local de usuarios Con esta opción los usuarios se administran de forma local en el ordenador instalado. Esto se recomienda en estaciones de trabajo autónomas (standalone) utilizadas por un solo usuario. En este caso, los datos de usuarios se administran por medio del archivo local `/etc/passwd`.

LDAP La administración de usuarios para todos los sistemas de la red se realiza de forma centralizada en un servidor LDAP.

NIS La administración de usuarios para todos los sistemas de la red se realiza de forma centralizada en un servidor NIS.

Samba La autenticación SMB se realiza con frecuencia en redes heterogéneas Linux y Windows.

Cuando se cumplan las condiciones previas, YaST abrirá un diálogo para seleccionar el método adecuado (figura 1.15 en la página siguiente). Si no dispone de ninguna conexión a una red, seleccione el modo de usuario local.

1.6.7. Configuración como cliente NIS

Si ha decidido desarrollar la administración de usuarios vía NIS, el siguiente paso consiste en configurar un cliente NIS. En este apartado se describe únicamente la configuración del lado del cliente. La configuración de un servidor NIS con YaST se describe en la capítulo **??** en la página ??.

En primer lugar se debe indicar si el cliente NIS dispone de una IP estática o dinámica vía DHCP (ver figura 1.16 en la página 31). En el último caso no es posible indicar un dominio NIS ni una dirección IP del servidor, porque estos valores también se asignan vía DHCP. Puede obtener información adicional sobre DHCP en la capítulo **??** en la página ??. Si el cliente dispone de una dirección IP estática, hay que anotar el domino NIS y el servidor.

El activar la opción de broadcast le permite buscar un servidor NIS en la red en caso de que el servidor indicado no conteste. También tiene la posibilidad de introducir varios dominios con un dominio predeterminado. Con la opción 'Añadir' puede también especificar varios servidores con función broadcast para cada dominio.

Figura 1.15: *Autenticación de usuarios*

La configuración de experto permite seleccionar la opción 'Sólo responder a host local' para evitar que otros ordenadores de la red puedan averiguar qué servidor es usado por su ordenador cliente. Utilice 'Servidor roto' para que se acepten también respuestas de un servidor en un puerto no privilegiado. Puede encontrar información adicional en la página de manual de `ypbind`.

1.6.8. Crear usuarios locales

Si no configura ninguna autenticación de usuarios basada en el servicio de nombres, se le ofrece la oportunidad de crear usuarios locales. Los datos de estos usuarios (nombre, login, contraseña, etc.) se guardan y gestionan en el sistema instalado.

Linux permite a varios usuarios trabajar simultáneamente. Para cada usuario debe existir una cuenta de usuario con la cual accede al sistema. Los archivos propios del usuario están protegidos del acceso de otros usuarios y no pueden ser modificados o borrados por estos. Además, cada usuario puede configurar su

Figura 1.16: *Configuración de un cliente NIS*

propio entorno de trabajo que encontrará inalterado cada vez que entre al sistema Linux.

Para crear cuentas de usuario se utiliza el diálogo de la figura 1.17 en la página siguiente. Debe indicar su nombre y apellidos y elegir también un nombre de usuario. Si no se le ocurre ningún nombre de usuario adecuado, puede crearlo automáticamente pulsando el botón 'Sugerencia'.

Por último hay que definir una contraseña para el usuario. Tiene que introducirla dos veces para su comprobación. El nombre de usuario indica al sistema su identidad y la contraseña garantiza que realmente se trata de Vd.

Aviso

Nombre de usuario y contraseña

Es muy importante recordar bien el nombre de usuario y la contraseña ya que para entrar al sistema necesitará estos dos datos con regularidad.

Aviso

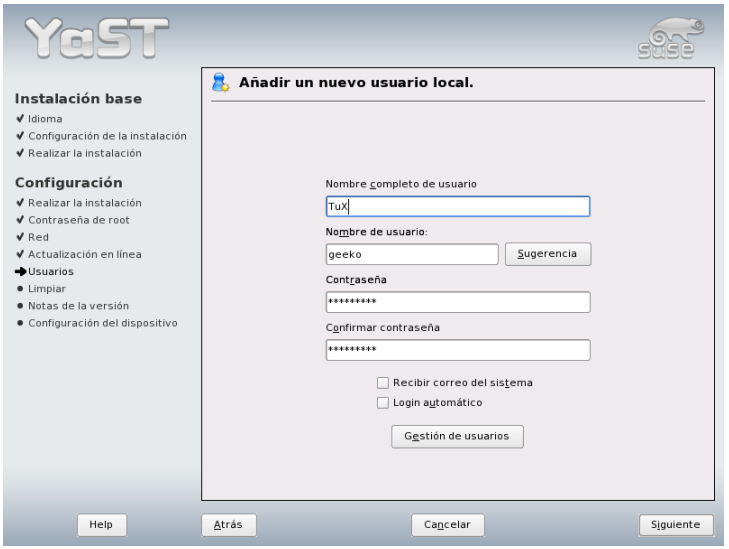

Figura 1.17: *Indicar nombre de usuario y contraseña*

Para una protección efectiva, la contraseña debe contener entre cinco y ocho caracteres, pudiendo contener hasta 128. Sin cargar ningún módulo especial sólo se usan los primeros ocho caracteres para la comprobación de la contraseña. Se distinguen mayúsculas y minúsculas; no se puede utilizar caracteres acentuados pero se permiten símbolos y las cifras del 0 a 9.

Para los usuarios locales pueden activarse dos opciones adicionales:

'Recibir correo del sistema' Para recibir los mensajes de los servicios del sistema debe marcar esta casilla. Normalmente sólo el usuario `root` los recibe. Se trata de una opción adecuada para aquellos usuarios que trabajen mucho tiempo con los programas sin entrar con frecuencia al sistema como `root`.

'Login automático' Esta opción sólo está disponible en caso de utilizar KDE como interfaz gráfica. Cuando está activada, el usuario actual entra automáticamente al sistema después de arrancar el ordenador. Resulta especialmente útil para un ordenador utilizado por una sola persona.

Aviso

El login automático suprime la autenticación por contraseña. *No* lo utilice para ordenadores con datos confidenciales a los que puedan acceder diferentes personas.

Aviso

1.6.9. Notas de versión

Después de configurar la autenticación de usuarios se mostrarán las notas de versión. Le aconsejamos que lea estas notas puesto que contienen información actual que aún no estaba disponible cuando se imprimió este manual. Si ha configurado una conexión a Internet y ha comprobado su funcionamiento con el servidor de SUSE, habrá obtenido la última versión de SUSE junto con información de última hora.

1.7. Configuración de hardware

Después de haber completado la instalación se mostrará un diálogo en el que puede configurar la tarjeta gráfica junto con diversos componentes de hardware conectados al sistema como impresoras o tarjetas de sonido. Si pulsa sobre los diferentes componentes puede iniciar la configuración del hardware. YaST detecta y configura el hardware de forma automática.

Puede realizar la configuración de los dispositivos externos más tarde, pero le recomendamos al menos configurar la tarjeta gráfica con los valores deseados. La propuesta estándar de YaST suele ser satisfactoria en la mayoría de los casos, pero las preferencias de imagen en pantalla (tales como resolución y tonalidad del color) varían mucho de un usuario a otro. Si quiere cambiar la configuración, seleccione la opción 'Tarjetas gráficas'. En la sección **??** en la página ?? se describen las ventanas de diálogo correspondientes. Una vez que YaST haya terminado de escribir los archivos de configuración, pulse 'Terminar' para finalizar la instalación de SUSE LINUX.

Figura 1.18: *Configuración de los componentes del sistema*

1.8. Login gráfico

Ahora SUSE LINUX está instalado. Si el login automático está activado, puede utilizarlo directamente sin pasos adicionales. En caso contrario, aparece en el monitor el login gráfico que puede ver en la figura 1.19 en la página siguiente. Introduzca el nombre de usuario definido anteriormente y su contraseña para entrar al sistema.

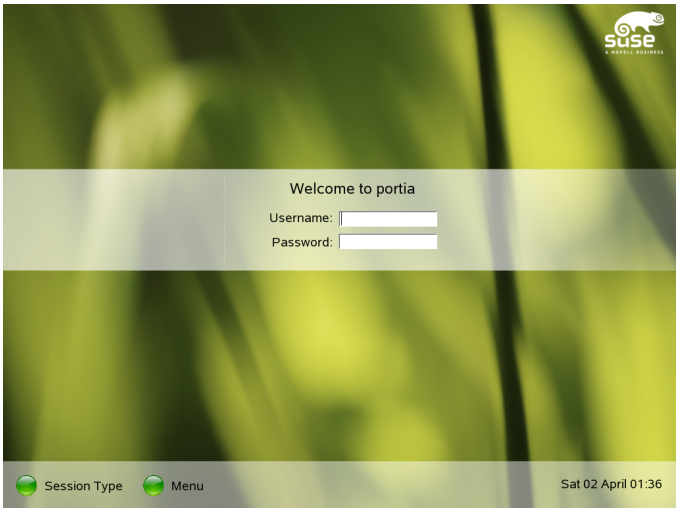

Figura 1.19: *Pantalla de inicio de sesión de KDM*

Configuración del sistema con YaST

YaST (Yet another Setup Tool), al que ya ha conocido durante la instalación, es también la herramienta de configuración de SUSE LINUX. Este capítulo explica la configuración del sistema con YaST, lo que comprende la mayoría del hardware, la interfaz gráfica de usuario, el acceso a Internet, la configuración de seguridad, la administración de usuarios y la instalación de programas así como las actualizaciones e información del sistema. Además incluye instrucciones para trabajar en modo texto con YaST.

Para llevar a cabo la configuración del sistema, YaST se sirve de diversos módulos. Dependiendo de la plataforma de hardware empleada y del software instalado, dispone de distintas posibilidades para acceder a YaST en el sistema instalado.

Si utiliza una de las interfaces gráficas de usuario KDE o GNOME, puede iniciar el centro de control de YaST a través del menú de SUSE ('Sistema' → 'YaST'). Además, KDE integra cada uno de los módulos de configuración de YaST en el centro de control KDE. Antes de que YaST se inicie, se le preguntará la contraseña de root. Esto es debido a que YaST requiere permisos de administrador para modificar los archivos del sistema.

Para iniciar YaST desde la línea de comandos, ejecute de forma sucesiva los comandos `su` (cambia al usuario `root`) y `yast2`. Si desea iniciar YaST en modo texto, introduzca `yast` en lugar de `yast2`. `yast` también puede utilizarse para iniciar el programa como `root` desde una consola virtual.

Sugerencia

Si desea cambiar el idioma en YaST, seleccione en el centro de control de YaST 'Sistema' → 'Escoger idioma'. Elija el idioma deseado y, a continuación, cierre el centro de control de YaST, salga de la sesión abierta y vuelva a entrar al sistema. La próxima vez que reinicie YaST, se habrá activado el nuevo idioma seleccionado.

Sugerencia

El inicio de YaST de forma remota resulta muy adecuado para las plataformas de hardware que no soportan una pantalla propia o para la administración remota desde otro ordenador. Para iniciar YaST a través de un terminal remoto, abra en primer lugar una consola e introduzca el comando `ssh -X root@<nombre_sistema>` para entrar al sistema remoto como usuario `root` y desviar la salida del servidor X a su terminal. Después de conectarse por medio de ssh, introduzca el comando `yast2` en el prompt del sistema remoto para iniciar YaST en modo gráfico y mostrarlo en el terminal local.

Para iniciar YaST en modo texto en otro sistema, ejecute `ssh root@<nombre_sistema>` e inicie YaST con el comando `yast`.

2.1. El Centro de Control de YaST

Si arranca en modo gráfico, aparecerá a continuación el centro de control de YaST (figura 2.1 en la página siguiente). La parte izquierda de la pantalla está dividida

en ‘Software’, ‘Hardware’, ‘Sistema’, ‘Dispositivos de red’, ‘Servicios de red’, ‘Seguridad y Usuarios’ y ‘Otros’. Al pulsar sobre los iconos podrá ver su contenido en la parte derecha de la pantalla. Por ejemplo, si pulsa ‘Hardware’ y después a la derecha ‘Sonido’, le aparecerá una ventana en la que podrá configurar la tarjeta de sonido. La configuración está dividida en varias partes. YaST le guía a través de todas ellas pulsando sobre ‘Siguiente’.

A la izquierda de la mayoría de los módulos aparece un texto de ayuda acerca del módulo cargado explicándole las entradas requeridas. Para acceder a la ayuda en módulos que no disponen de un marco de ayuda, pulse F1 o seleccione ‘Ayuda’ en el menú. Una vez que haya completado la configuración, pulse ‘Finalizar’ en el último diálogo de configuración para guardarla.

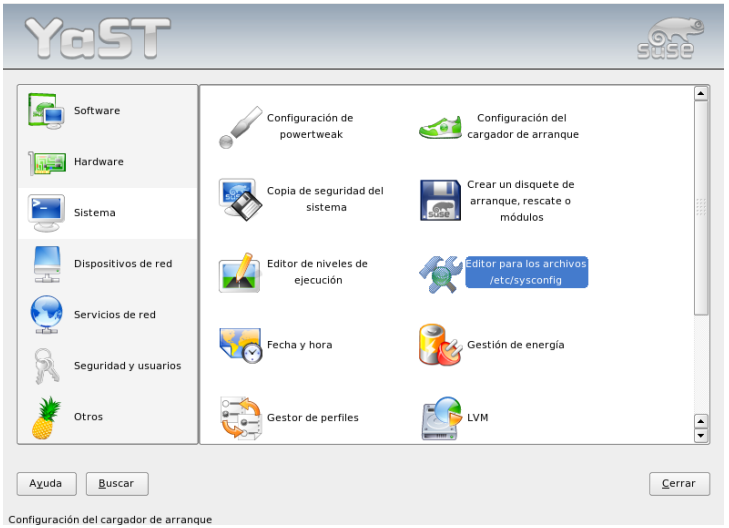

Figura 2.1: *El Centro de Control de YaST*

2.2. Software

2.2.1. Instalar y desinstalar software

Este módulo permite instalar, borrar y actualizar el software del ordenador. En Linux el software se presenta en forma de paquetes. Un paquete contiene todo lo que pertenece a un programa completo, es decir, el programa en sí, los archivos de configuración y la documentación correspondiente. Debido a que en Linux el código fuente de un programa suele estar disponible, normalmente existe un paquete correspondiente con las fuentes del programa. Estas fuentes no se necesitan para trabajar con el programa, pero en ciertos casos instalarlas puede resultar interesante porque le permiten crear una versión del programa a su medida.

Hay ciertos paquetes que dependen funcionalmente de otro. En tal caso, el programa de un paquete sólo puede funcionar correctamente cuando otro paquete también está instalado. Aparte de este requerimiento, hay también paquetes que exigen la existencia de otros sólo para poder ser instalados. La razón es que necesitan ejecutar ciertas rutinas que son proporcionadas por los paquetes requeridos. Para instalar tales paquetes hay que observar un orden determinado de instalación. Además a veces existen varios paquetes para un mismo propósito. Si estos paquetes utilizan los mismos recursos del sistema, no pueden ser instalados simultáneamente (conflicto de paquetes). Las dependencias y conflictos entre varios paquetes pueden formar cadenas largas y difíciles de analizar. El asunto se vuelve más complicado cuando la buena armonía de los programas depende también de sus versiones.

Todas las condiciones se han de cumplir en todo momento independientemente de si instalamos, desinstalamos o actualizamos el sistema. Afortunadamente YaST incorpora el gestor de paquetes, una herramienta realmente potente para comprobar las dependencias. El gestor de paquetes realiza un reconocimiento de sistema, mostrando todos los paquetes que ya están instalados en el mismo. Al seleccionar paquetes adicionales para su instalación, el gestor de paquetes considera las dependencias y las resuelve añadiendo automáticamente otros paquetes (si hace falta). Si selecciona paquetes que están en conflicto, el gestor de paquetes lo notifica y propone una solución para resolver el conflicto. Lo mismo ocurre cuando se haya seleccionando un paquete para ser borrado del sistema y otros paquetes lo requieran.

Aparte de los aspectos técnicos, el gestor de paquetes proporciona una vista estructurada sobre todos los paquetes disponibles en SUSE LINUX. Esta vista o resumen de paquetes se realiza con filtros que reducen la cantidad de paquetes a unos cuantos grupos temáticos.

El gestor de paquetes

Para modificar el contenido de software en su sistema, seleccione 'Instalar/desinstalar software' en el centro de control de YaST. La ventana de diálogo del gestor de paquetes se muestra en la figura 2.2 en esta página.

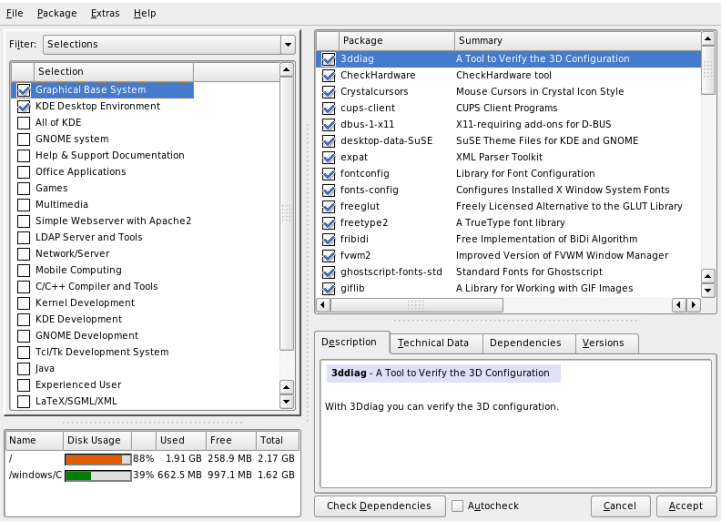

Figura 2.2: *El gestor de paquetes de YaST*

La ventana de filtros

El gestor de paquetes ofrece diferentes métodos de filtrado que dividen los paquetes por categorías y limitan el número de paquetes mostrados. La ventana de filtros está situada en la parte inferior izquierda de la barra de menús y se encarga de controlar y mostrar varios métodos de filtrado. El contenido de la casilla de selección de filtros determina lo que se muestra en la parte inferior de la ventana de filtros. Pulse con el ratón en la caja de selección de filtros para seleccionar un filtro de la lista de filtros disponibles.

El filtro de selecciones Al iniciar el gestor de paquetes, el filtro de 'Selecciones' está activado. Este filtro agrupa los programas en función de su finalidad,

como ”Multimedia” u ”Ofimática”. Los distintos grupos del filtro ‘Selecciones’ aparecen enumerados bajo la caja de selección. Los paquetes ya instalados en el sistema están preseleccionados. Pulsando con el ratón en la casilla de estado al principio de cada línea puede cambiar la marca de estado de una selección. Para seleccionar un estado directamente, pulse en la selección con el botón derecho del ratón y utilice el menú contextual. La ventana de paquetes individuales en la parte derecha muestra todos los paquetes que pertenecen a la selección actual y en ella es posible seleccionar o deseleccionar paquetes individuales.

El filtro de grupos de paquetes Otra posibilidad de filtrado consiste en utilizar los ‘Grupos de paquetes’. Se trata de un filtro con una cierta orientación técnica, pensado para usuarios que ya conocen el conjunto de paquetes de SUSE LINUX. Los programas se organizan por materias como ”aplicaciones”, ”desarrollo” o ”hardware” en una estructura en forma de árbol en la parte izquierda. Cuanto más se abra este árbol, más se especifica el tema y la cantidad de paquetes que se muestra en la parte derecha se reduce.

Este filtro también permite mostrar *todos* los paquetes en orden alfabético. Para ello seleccione en el nivel más alto ‘zzz todo’. Dado que SUSE LINUX incorpora muchos paquetes, es posible que la creación de esta lista lleve algún tiempo.

La función de búsqueda La forma más sencilla de encontrar un determinado paquete es utilizar la función ‘Buscara’. Mediante los criterios de búsqueda adecuados, es posible conseguir que en la lista de paquetes encontrados aparezca sólo un paquete. Para ello introduzca una cadena de caracteres y determine dónde debe realizarse la búsqueda: en el nombre del paquete, su descripción o en las dependencias del paquete. Los usuarios avanzados pueden introducir comodines o expresiones regulares y buscar en las dependencias de paquetes en los apartados ”Proporciona” y ”Requiere”. Por ejemplo, esta función puede emplearse para determinar qué paquete contiene una librería determinada.

Sugerencia

Búsqueda rápida

Además del filtro 'Buscar', existe una búsqueda rápida en todas las listas del gestor de paquetes. Para ello basta con introducir la letra inicial del nombre de un paquete y el cursor salta al primer paquete de la lista cuyo nombre comience con este carácter. Para este método de búsqueda el cursor ha de estar en la lista (pinchando con el ratón en la lista).

Sugerencia

Idiomas Algunos de los paquetes de SUSE LINUX están disponibles en una versión específica para un idioma determinado. Estos paquetes contienen, por ejemplo, textos traducidos para las interfaces de usuario de los programas, documentación y tipos de letra. Este filtro muestra en la ventana de la izquierda una lista de los idiomas soportados en SUSE LINUX. Al seleccionar uno de ellos, la ventana de la derecha muestra todos los paquetes disponibles para ese idioma. De entre estos paquetes, todos los que sean adecuados para la selección de software actual se marcan automáticamente para su instalación.

Nota

Debido a que los paquetes específicos para un idioma pueden depender de otros paquetes, es posible que el gestor de paquetes seleccione además otros paquetes para la instalación.

Nota

Resumen de la instalación Después de haber seleccionado paquetes para instalar, actualizar o eliminar, puede ver un resumen de la instalación y saber con exactitud qué pasará con cada paquete en cuanto pulse 'Aceptar'. Mediante la secuencia de casillas que se encuentran a la izquierda puede filtrar los paquetes en función de las acciones. Si sólo quiere comprobar qué paquetes ya están instalados, desactive todas las casillas (excepto 'Mantener') directamente después del inicio del gestor de paquetes.

El estado de los paquetes dentro de la ventana de los paquetes individuales se cambia en la forma habitual. No obstante, puede que después de haber cambiado su estado, un paquete ya no coincida con los criterios de búsqueda. Para eliminar estos paquetes de la lista pulse 'Actualizar lista'.

La ventana de paquetes

El conjunto de paquetes que se muestra en la lista de paquetes individuales depende del filtro seleccionado. Por ejemplo, si el filtro 'Selecciones' está activo, se muestran los paquetes que pertenecen a la selección actual.

Hay un estado lógico asignado a cada paquete que determina lo que pasará con ese paquete, como "Instalar" o "Borrar". Como en el filtro de selecciones, este estado se muestra al comienzo de la línea con un símbolo. Aquí también es posible cambiar de estado mediante sucesivas pulsaciones del ratón o pulsando con el botón derecho sobre el nombre del paquete y seleccionándolo directamente desde el menú desplegable. Dependiendo de la situación global, algunos estados pueden no estar disponibles. Evidentemente, no es posible seleccionar el estado "Borrar" para un paquete que aún no esté instalado. Para consultar los estados posibles y los correspondientes símbolos, seleccione en el menú 'Símbolos' → 'Ayuda'.

El gestor de paquetes contempla los siguientes estados para el paquete:

No instalar Este paquete no está instalado y tampoco se instalará.

Instalar Este paquete no está instalado, pero se instalará.

Mantener Este paquete ya está instalado y se mantiene sin cambios.

Actualizar Este paquete ya está instalado y será reemplazado por la versión procedente del medio de instalación.

Borrar Este paquete ya está instalado y se borrará.

Tabú — no instalar nunca Este paquete no está instalado y no se instalará bajo ninguna circunstancia. Se tratará como si no existiera en ningún medio de instalación. Por ejemplo, si un paquete se debería añadir automáticamente para resolver las dependencias, con "Tabú" se puede evitar que se instale. Los conflictos que resulten a raíz de ello se han de resolver manualmente. Por este motivo, "Tabú" es una opción para expertos.

Protegido Este paquete está instalado y no se debe modificar porque puede haber dependencias no resueltas con otros paquetes. Los paquetes de terceros (sin firma de SUSE) automáticamente reciben este estado para que no sean sobreescritos por paquetes más nuevos que se encuentren en el medio de instalación. Esto podría provocar conflictos entre paquetes que deberían resolverse manualmente.

Instalar automáticamente El gestor de paquetes ha seleccionado este paquete automáticamente porque es requerido por otro paquete (solución de las dependencias entre paquetes). Para deseleccionar uno de estos paquetes, es posible que tenga que utilizar el estado ”Tabú”.

Actualizar automáticamente Este paquete ya está instalado. Sin embargo, otro paquete requiere una versión posterior del mismo, por lo que será actualizado.

Borrar automáticamente Este paquete ya se encuentra instalado, pero existe un conflicto de paquetes que obliga a borrarlo. Esto puede ser el caso cuando otro paquete nuevo reemplaza el existente.

Instalar automáticamente (después de seleccionar)
Este paquete ha sido seleccionado automáticamente para su instalación porque forma parte de una selección predefinida (como por ejemplo ”Multimedia” o ”Desarrollo”).

Actualizar automáticamente (después de seleccionar)
Este paquete ya está instalado, pero existe una versión más nueva en el medio de instalación que forma parte de una selección (como ”Multimedia” o ”Desarrollo”). Por eso se selecciona y actualiza automáticamente.

Borrar automáticamente (después de seleccionar)
Este paquete ya está instalado, pero una de las selecciones predefinidas (por ejemplo ”Multimedia” o ”Desarrollo”) requiere que sea borrado.

Adicionalmente es posible determinar si las fuentes de un programa se deben instalar junto con él. Para realizar esta instalación, marque la casilla que se encuentra en el extremo derecho de la línea de descripción del paquete. Esta opción también puede seleccionarse en el menú ‘Paquete’.

Instalar fuente El código fuente se instalará.

No instalar fuente El código fuente no se instalará.

El color de la letra que se utiliza dentro de la ventana de paquetes proporciona información adicional. Aquellos paquetes ya instalados para los que existe una nueva versión en el medio de instalación, se muestran en letra azul. En cambio, cuando la versión instalada en el sistema es más reciente que la del medio de instalación, se utiliza el color rojo. Puesto que la enumeración de los paquetes no

siempre es continua, es posible que no se pueda determinar la actualidad del paquete. Por eso la información dada no es correcta al cien por cien, pero al menos es suficiente para indicar qué paquetes pueden problemáticos. Para ver exactamente el número de versión, utilice la ventana de información.

La ventana de información

En la parte inferior derecha se encuentra una ventana con pestañas que le proporciona información sobre los paquetes seleccionados. Al iniciarla, la descripción del paquete actual está activada. Pulse las pestañas para obtener información técnica sobre el paquete (tamaño, grupo de paquetes, etc.), la lista de dependencias y la versión.

La ventana de recursos

Durante el proceso de selección del software, la ventana de recursos muestra el uso de todos los sistemas de archivos montados tal y como sería después de habar acabado la instalación. La ocupación se muestra en un diagrama de barras de color. Verde significa que hay aún suficiente espacio. La barra pasa a tener un color rojo conforme se va utilizando el espacio en disco. Los valores que se muestran son virtuales, ya que la instalación aún no se ha realizado. Cuando el espacio esté totalmente agotado, aparece una ventana de aviso.

La barra de menús

La barra de menús en la parte superior de la ventana también permite acceder a la mayoría de las funciones ya explicadas. Ésta contiene cuatro menús:

Archivo La opción 'Exportar' en 'Archivo' permite crear una lista de todos los paquetes instalados y grabarla en un archivo de texto. Es muy práctica para reproducir en otro momento o en otro sistema una selección de software idéntica. Con la función 'Importar'puede cargar un archivo creado de este modo y generar así una selección de paquetes idéntica a la de otro sistema. En ambos casos puede decidir libremente dónde desea guardar el archivo o aceptar la propuesta del sistema.

La opción 'Salir – desechar cambios' sirve para salir del gestor de paquetes, desechando todos los cambios que haya realizado desde el inicio del gestor. En cambio, para grabar las modificaciones, seleccione 'Salir – guardar cambios'. Ahora todas las modificaciones se llevan a cabo y finalmente el programa se termina.

Paquete Las opciones dentro del menú 'Paquete' siempre se refieren al paquete actual dentro de la ventana de paquetes individuales. Aunque aparecen todos los estados que un paquete puede tener, sólo puede seleccionar los estados posibles y relevantes para ese paquete. Las casillas ofrecen también la posibilidad de instalar las fuentes junto con el programa. La opción 'Todos los de la lista' abre un submenú que contiene nuevamente todos los estados de paquete. Una selección en esta lista no se refiere al paquete actual, sino a *todos* los paquetes de la lista.

Extras El menú 'Extras' incorpora opciones para manejar dependencias y conflictos de paquetes. Después de haber seleccionado manualmente paquetes para su instalación, un clic sobre 'Mostrar cambios automáticos de paquetes' muestra una lista de los paquetes seleccionados automáticamente por el gestor de paquetes para solucionar dependencias. Si aún existen conflictos de paquetes sin resolver, aparece una ventana con propuestas para solucionarlos.

Cuando activa la opción "Ignorar" para los conflictos de paquetes, dicha opción se guarda de forma permanente en el sistema. Si no fuera así, tendría que poner el mismo paquete en estado "Ignorar" cada vez que entrase al gestor de paquetes. Para desactivar esta opción utilice 'Restablecer conflictos de dependencias ignorados'.

Ayuda 'Resumen' dentro del menú 'Ayuda' muestra un resumen del funcionamiento del gestor de paquetes. Una explicación detallada de los estados de paquetes y sus símbolos se encuentra bajo la opción 'Símbolos'.Para conocer el uso del programa con 'Teclas' en lugar del ratón,pulse la opción correspondiente para obtener una explicación de las teclas abreviadas.

Comprobar dependencias

En la parte inferior derecha de la ventana de información se encuentra un botón llamado 'Comprobar dependencias' y a su lado una casilla llamada 'Comprobación automática'. Pulsando el botón, el gestor de paquetes comprueba si existen dependencias no resueltas o inconsistencias para la selección de paquetes actual. Para resolver las dependencias, los paquetes que faltan se seleccionan automáticamente. En caso de conflictos, el gestor de paquetes abre una ventana para visualizarlos y muestra en ella posibles soluciones.

Si se activa 'Comprobación automática', la comprobación se ejecuta cada vez que se cambia el estado de un paquete. Por una parte es una opción útil porque se vigila permanentemente que no haya conflictos de paquetes, pero por otra, la com-

probación cuesta tiempo de cálculo y el uso del gestor de paquetes se puede ralentizar. Por este motivo, la comprobación automática no está preseleccionada. En cualquier caso siempre se realiza dicha comprobación cuando se termina el diálogo con 'Aceptar'.

En el siguiente ejemplo los paquetes `sendmail` y `postfix` no se pueden instalar simultáneamente. En la figura 2.3 en la página siguiente puede ver el mensaje de conflicto donde se requiere una decisión. `postfix` ya está instalado, así que puede renunciar a la instalación de `sendmail`, eliminar `postfix` o correr el riesgo e ignorar el conflicto.

Aviso

Tratamiento de conflictos entre paquetes

A la hora de procesar los conflictos entre paquetes, le recomendamos aceptar las sugerencias del gestor de paquetes de YaST. En caso contrario, el conflicto podría repercutir negativamente en la estabilidad y funcionalidad de su sistema.

Aviso

2.2.2. Cambiar la fuente de instalación

YaST es capaz de trabajar con diferentes fuentes de instalación que pueden seleccionarse directamente para realizar procesos de instalación o actualización. Cuando se inicia el módulo aparece una lista de todas las fuentes de instalación registradas hasta el momento. Después de una instalación normal desde un CD, esta lista sólo contiene el CD como fuente. Con el botón 'Añadir' puede incorporar otras fuentes de instalación a esta lista; no sólo medios extraíbles como CDs y DVDs, sino también conexiones de red como NFS y FTP. Los directorios en discos locales son también medios de instalación válidos (ver el texto de ayuda sobre YaST).

Todas las fuentes de instalación aquí registradas disponen de un estado de activación que se muestra en la primera columna de la lista. Pulse 'Activar o desactivar' para cambiar dicho estado. Cuando se realiza una instalación o actualización, YaST selecciona la entrada más adecuada de entre las fuentes de instalación activadas. Al salir del módulo mediante 'Cerrar', la configuración actual se graba y se utilizará para los módulos de configuración 'Instalar/desinstalar software' y 'Actualización del sistema'.

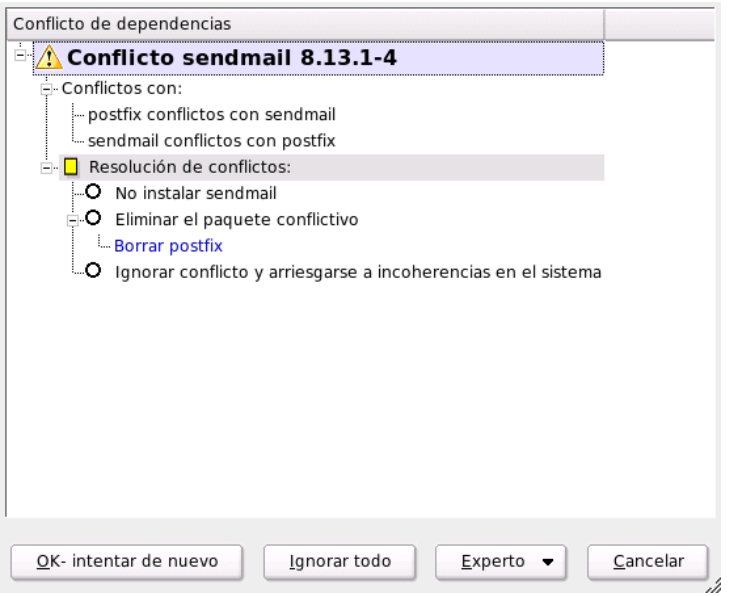

Figura 2.3: *Gestión de conflictos del gestor de paquetes*

2.2.3. YaST Online Update

La actualización en línea de YaST (YOU) permite la instalación de actualizaciones y mejoras importantes. Los parches (patches) correspondientes se encuentran disponibles en el servidor FTP de SUSE.

En el apartado 'Fuente de instalación' puede elegir entre diferentes servidores. Al seleccionar uno de ellos, la URL correspondiente aparece en la casilla de texto inferior donde puede ser editada. Otra posibilidad consiste en introducir una URL local como "file:/mi/ruta" (o sencillamente "/mi/ruta"). Pulse 'Nuevo servidor' para ampliar la lista con nuevos servidores. Otra opción es 'Editar servidor' que permite modificar la configuración del servidor seleccionado actualmente.

Al iniciar el módulo, la opción 'Seleccionar parches manualmente' está activada, permitiéndole seleccionar cada parche individualmente. Desactive esta opción para instalar todos los paquetes de actualización disponibles. No obstante, dependiendo del ancho de banda y de la cantidad de datos, el tiempo de carga en este caso puede ser muy largo.

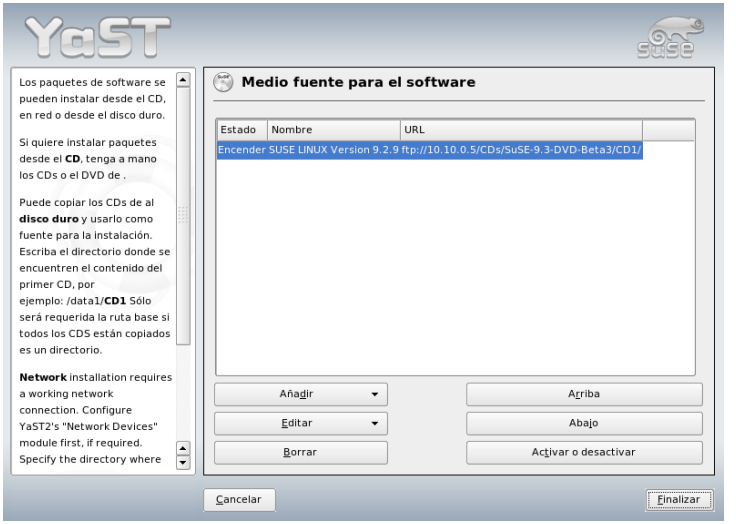

Figura 2.4: *Cambiar la fuente de instalación*

Si activa 'Cargar todos los parches del servidor', bajarán del servidor todos los parches, paquetes de instalación y descripciones disponibles. Si esta opción no está activa (configuración predeterminada), sólo se descargarán los paquetes que aún no están instalados en el sistema.

Asimismo existe la posibilidad de actualizar el sistema automáticamente. Con 'Configurar actualización totalmente automática...' se configura un proceso que busca e instala actualizaciones periódicamente. Aunque este proceso está totalmente automatizado, evidentemente es necesario poder establecer una conexión con el servidor de actualizaciones cuando sea preciso.

Pulse 'Siguiente' para iniciar la actualización. En el caso de una actualización manual, al realizar esta acción todos los parches disponibles se cargan y el gestor de paquetes se inicia (ver sección 2.2.1 en la página 40). En el gestor de paquetes se activa el filtro para parches YOU, permitiendo la selección de los parches que se han de instalar. Los parches pertenecientes a las categorías security y recommended están preseleccionados siempre que los paquetes correspondientes ya estén instalados en el sistema. Se recomienda aceptar esta propuesta.

Después de seleccionar los parches, pulse 'Aceptar' en el gestor de paquetes. Posteriormente todos los parches seleccionados se descargan del servidor y se insta-

lan en el ordenador. Dependiendo de la conexión al servidor y de la potencia del ordenador, este proceso puede llevar cierto tiempo. Los posibles errores se muestran en una ventana y es posible omitir el paquete que ocasiona el error. Algunos parches abren una ventana antes de la instalación para mostrar información detallada.

Durante la carga e instalación de los parches, puede seguir el proceso en la ventana de protocolo. Salga con 'Terminar' del diálogo de YOU después de terminar la instalación de todos los parches. Mediante 'Borrar fuentes después de la instalación' puede borrar las fuentes que haya bajado si ya no las necesita. Posteriormente se ejecuta SuSEconfig para ajustar la configuración del sistema en caso necesario.

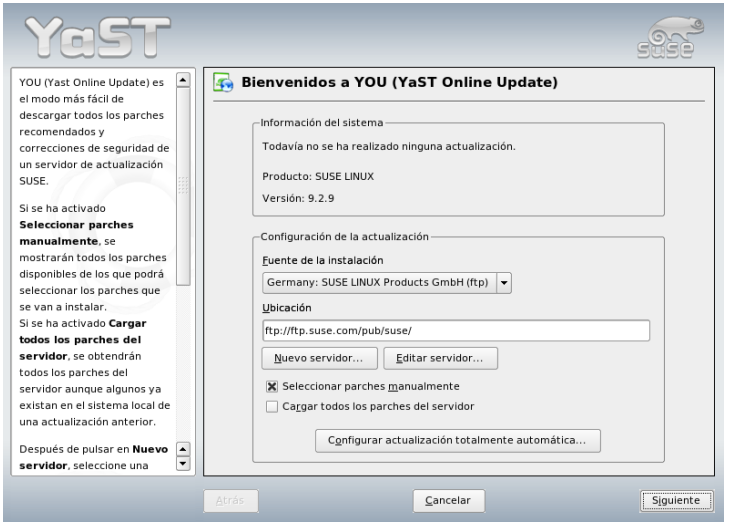

Figura 2.5: *YaST Online Update*

2.2.4. Actualización del sistema

Este módulo le permite pasar su sistema actual a una versión más nueva. Durante el uso del sistema sólo se pueden actualizar aquellos componentes que no están ejecutándose. Por eso no se puede actualizar el sistema base SUSE LINUX

sino sólo aplicaciones. Para actualizar todo el sistema hace falta arrancar desde el medio de instalación (CD). En el momento de seleccionar el modo de instalación dentro de YaST, seleccione 'Actualizar un sistema ya existente' en lugar de 'Nueva instalación'.

La actualización se parece bastante a la instalación nueva del sistema. YaST averigua primero el estado actual de su sistema, determina una estrategia de actualización adecuada y presenta los resultados en un diálogo de propuestas. Al igual que durante la instalación, también en este caso puede seleccionar las diferentes opciones con el ratón para realizar modificaciones individuales. La mayoría de las opciones como 'Idioma' y 'Distribución de teclado' ya se explicaron para la instalación (vea la sección 1.3 en la página 8). A continuación sólo se explican opciones específicas de la actualización.

Seleccionado para la actualización

Si existen varias versiones de SUSE LINUX instaladas en su sistema, aquí puede seleccionar la partición que quiere actualizar. El cuadro de selección muestra todas las particiones que pueden ser actualizadas.

Opciones de actualización

Aquí puede definir el método de actualización del sistema. Hay dos opciones disponibles.

Actualizar con instalación de nuevo software
: Para actualizar todo el sistema al estado actual del software, elija una de las selecciones predefinidas. Son las mismas selecciones que se ofrecen en la instalación regular. Por eso es posible que se instalen también paquetes nuevos que aún no se encuentran instalados.

Actualizar sólo paquetes instalados Esta opción sólo actualiza paquetes que ya estén disponibles en el sistema; no se instalan programas nuevos.

Otro opción es 'Borrar paquetes sin mantener' para borrar todos aquellos paquetes que ya no forman parte de la versión nueva. Esta opción está preseleccionada para evitar que paquetes antiguos ocupen espacio en el disco duro.

Paquetes

'Paquetes' inicia el gestor de paquetes para tener la opción de seleccionar o quitar paquetes individuales de la actualización. Utilice la comprobación de dependencias para visualizar y resolver los conflictos entre paquetes. El manejo del gestor de paquetes se explica detalladamente en la sección 2.2.1 en la página 40.

Copia de seguridad

A la hora de actualizar el sistema, es posible que se reemplacen los archivos de configuración de algunos paquetes por archivos nuevos. Estos archivos pueden haberse modificado en su sistema y para no perderlos, se crea una copia de seguridad de los mismos. El presente diálogo permite determinar el alcance de estas copias.

Importante

Alcance de la copia de seguridad

Estas copias de seguridad no engloban todo el software, sino sólo los archivos de configuración correspondientes.

Importante

Información importante sobre la actualización

La actualización del sistema es un asunto de gran complejidad técnica. En primer lugar, YaST comprueba la versión actual de cada paquete y a continuación determina la acción que debe realizarse para sustituir dicha versión por una nueva. Además, YaST intenta conservar en cada paquete las configuraciones personales en la medida de lo posible. Puede ocurrir en algunos casos que, después de la actualización de una determinada configuración, ocurran problemas debido a que la configuración anterior no funcione como se esperaba con la nueva versión o porque se han producido inconsistencias que no se pudieron prever entre distintas configuraciones.

Cuanto más antigua es la versión que va a actualizarse y más difiere la configuración del paquete de configuración estándar, más complejo resulta el proceso de actualización. En raras ocasiones en las que no se puede procesar correctamente una configuración anterior, es necesario volver a crear una configuración nueva. Por ello es conveniente que guarde la configuración anterior antes de proceder a la actualización.

2.2.5. Comprobación de medios

Si surgen problemas con los medios de instalación de SUSE LINUX, este módulo le permite comprobar los CDs o DVDs. En algunos casos muy raros, algunos dispositivos podrían tener problemas para leer ciertos medios correctamente, si bien es más probable que esto suceda con medios de ”fabricación propia”. Para comprobar si un CD o DVD de SUSE LINUX está libre de fallos, introduzca el medio

en el lector correspondiente y ejecute este módulo. Al pulsar 'Iniciar', YaST comprobará la suma de control MD5 del medio. Esto puede llevar unos minutos. En caso de que la comprobación dé como resultado algún error, se recomienda no utilizar ese medio para la instalación.

2.3. Hardware

El nuevo hardware debe conectarse e instalarse siguiendo las recomendaciones del fabricante. Encienda los periféricos externos tales como la impresora y el módem y ejecute el módulo de YaST correspondiente. YaST detecta de forma automática una gran parte de los dispositivos y componentes y muestra sus datos técnicos. Si la detección automática falla, YaST le proporciona una lista de dispositivos (por ejemplo modelo/fabricante) en la que puede seleccionar el dispositivo adecuado. Consulte la documentación de su hardware si la información impresa en el dispositivo no es suficiente.

Importante

Nombres de modelos

Si el modelo no está incluido en la lista de dispositivos, pruebe un modelo que posea una descripción similar al suyo. Por desgracia, en algunas ocasiones es absolutamente necesario introducir las especificaciones exactas para su dispositivo, ya que las descripciones generales dadas no garantizan la compatibilidad con su hardware.

Importante

2.3.1. Unidades de CD-ROM y DVD

Durante la instalación se integran todas las unidades de CD-ROM detectadas en el sistema instalado mediante las entradas correspondientes en el archivo `/etc/fstab` y se crean los subdirectorios `/media`. Con este módulo de YaST también puede integrar en el sistema unidades montadas posteriormente.

Después de activar el módulo se presenta una lista con todas las unidades detectadas. Marque la unidad nueva y pulse en 'Finalizar'. La nueva unidad está ahora integrada en el sistema y se puede utilizar.

2.3.2. Impresora

Puede obtener información detallada sobre la impresión en Linux en el capítulo **??** en la página ??, en el que se describe el tema de la impresión de manera general.

YaST configura la impresora automáticamente o bien ofrece diálogos de configuración para ayudar al usuario a configurar la impresora de forma manual. Una vez configurada la impresora, el usuario puede imprimir desde la línea de comandos o configurar las aplicaciones para utilizar el sistema de impresión. La sección **??** en la página ?? contiene una descripción detallada de la configuración de impresoras con YaST.

2.3.3. Controlador de disco duro

YaST suele configurar el controlador de disco duro de su sistema durante la instalación. Si integra controladores adicionales, puede realizar la instalación con este módulo de YaST. Aquí también puede cambiar la configuración existente, lo que por otra parte no debería ser necesario.

La ventana de diálogo ofrece una lista con todos los controladores de discos duros detectados y permite asignar los módulos de kernel adecuados con parámetros específicos. Con 'Probar la carga del módulo' puede comprobar si funciona la configuración actual antes de grabarla definitivamente en el sistema.

Aviso

Configuración del controlador de disco duro

Esta es una herramienta para expertos. Si efectúa una configuración errónea, puede que el sistema no vuelva a arrancar. En cualquier caso, utilice siempre la opción de prueba.

Aviso

2.3.4. Información del hardware

YaST realiza un reconocimiento de hardware para la configuración de componentes de hardware. Los datos técnicos detectados se muestran en una ventana propia. Esto es especialmente útil si por ejemplo quiere realizar una consulta a nuestro equipo de soporte, para lo que necesita tener información sobre su hardware.

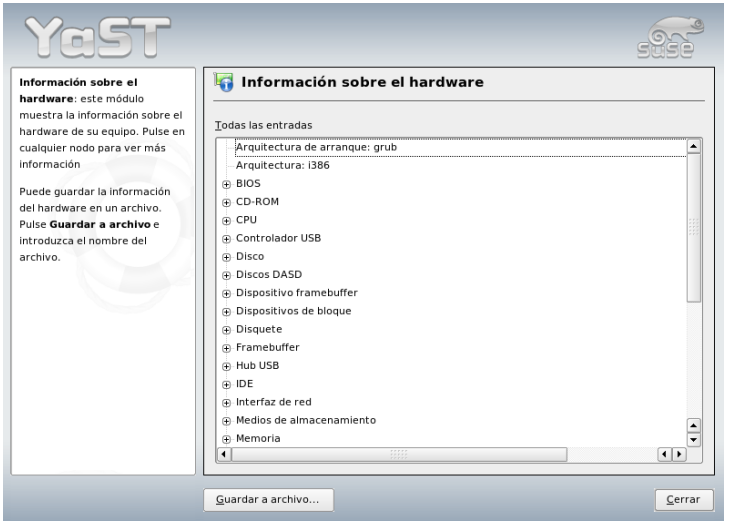

Figura 2.6: *Mostrar información del hardware*

2.3.5. Módulo DMA

Este módulo le permite activar o desactivar el modo DMA para el disco duro (IDE) y el lector de CD/DVD (IDE). En dispositivos SCSI este módulo no funciona. Con un modo DMA activado el rendimiento del sistema puede mejorar bastante, ya que se aumenta la velocidad de transferencia de datos.

Durante la instalación, el kernel actual de SUSE LINUX activa DMA automáticamente para los discos duros pero no lo activa para los lectores de CD, ya que en el pasado a veces hubo problemas con los CD-ROM cuando el DMA se activaba para todos los dispositivos. El módulo para la configuración de DMA le permite al usuario decidir si quiere utilizar DMA también para el CD-ROM y así mejorar la tasa de transferencia. Igualmente es posible *desactivar* DMA para los discos duros en caso de tener problemas con ellos.

Importante

DMA (=**D**irect **M**emory **A**ccess) significa acceso directo a la memoria. Es decir, los dispositivos pueden transferir sus datos directamente a la memoria sin el desvío por el procesador.

Importante

2.3.6. Escáner

Si el escáner está conectado y activado, debería ser detectado automáticamente cuando se inicia el módulo de YaST. En este caso debería aparecer un diálogo para la instalación del escáner. Si no ha sido detectado, deberá recurrir a la configuración manual. Si, por el contrario, ya tiene varios escáneres instalados, aparecerá un listado con los escáneres existentes, los cuales pueden ser cambiados o eliminados. Puede agregar un nuevo dispositivo con 'Añadir'.

Después se realizará una instalación con una configuración estándar. Si la instalación ha tenido éxito, aparecerá un mensaje. A continuación puede probar su escáner introduciendo un documento y pulsando en 'Probar'.

Escáner no detectado

Tenga en cuenta que sólo los escáneres soportados pueden ser detectados automáticamente. Los escáneres de red no se pueden detectar automáticamente. Para la configuración manual, debe distinguir entre escáner USB, SCSI o escáner de red.

Escáner USB Aquí debe introducir el fabricante y el modelo. YaST intentará cargar el módulo USB. Si el escáner es muy nuevo, puede que los módulos no sean cargados automáticamente. En este caso deberá acudir al diálogo que permite cargar los módulos USB manualmente. Consulte los textos de ayuda de YaST para obtener más información al respecto.

Escáner SCSI Especifique el dispositivo (ej. `/dev/sg0`). Un escáner SCSI no puede conectarse o desconectarse mientras el sistema está en funcionamiento. Debe apagar primero el sistema.

Escáner de red Debe introducir la dirección IP o el nombre del servidor. Para obtener información adicional sobre la configuración de un escáner de red, consulte el artículo de la base de datos de soporte *Scanner under Linux*

(`http://portal.suse.com/sdb/en/index.html`, término de búsqueda `scanner`).

Si el escáner no ha sido detectado, posiblemente el dispositivo no esté soportado. Sin embargo, a veces incluso los escáneres soportados no son detectados. La selección manual puede ser la solución; en este caso consiga más información sobre su escáner. Una vez hecho esto, identifique el modelo en la lista y selecciónelo. Si no lo encuentra pulse en 'Cancel'. Puede encontrar más información sobre cómo trabajar con escáneres en Linux en `http://cdb.suse.de` o `http://www.mostang.com/sane`.

Aviso

Configuración manual del escáner

Sólo debe configurar el escáner manualmente si está seguro de cómo hacerlo. Una configuración incorrecta puede dañar el hardware.

Aviso

Solución de errores

El escáner puede no ser detectado por alguna de las siguientes causas:

- El escáner no está soportado. Puede encontrar una lista de los dispositivos compatibles con Linux en `http://cdb.suse.de`.
- La controladora SCSI no ha sido instalada correctamente.
- Problemas con el puerto SCSI.
- El cable SCSI sobrepasa la longitud permitida.
- El escáner tiene una controladora SCSI Light que no está soportada por Linux.
- El escáner podría ser defectuoso.

Aviso

Los escáneres SCSI no pueden ser conectados o desconectados mientras el sistema está en funcionamiento. Apague primero el ordenador.

Aviso

Puede encontrar más información sobre los escáneres en el capítulo sobre `kooka`.

2.3.7. Sonido

Al iniciar la herramienta de configuración de sonido, YaST intentará detectar la tarjeta de sonido. Puede configurar una o más tarjetas de sonido. Si desea utilizar más de una tarjeta, seleccione primero aquella que desea configurar. Con el botón 'Configurar' volverá al menú de 'Configuración'. El botón 'Editar' le permite editar las tarjetas ya configuradas. La opción 'Finalizar' graba la actual configuración y completa la configuración del sonido.

Si YaST no puede detectar la tarjeta de sonido automáticamente, pulse 'Añadir tarjeta de sonido' en el menú 'Configuración de sonido' para abrir un diálogo en el que seleccionar una tarjeta de sonido y un módulo. Puede consultar una lista de las tarjetas de sonido soportadas por ALSA con sus módulos de sonido correspondientes en `/usr/share/doc/packages/alsa/cards.txt` y en `http://www.alsa-project.org/~goemon/`. Una vez que haya realizado la selección, pulse 'Siguiente' para volver a la 'Configuración'.

Configuración

En la primera pantalla de este diálogo puede elegir el nivel de configuración. Si selecciona el menú 'Configuración rápida', no se requerirán más que los pasos básicos para la configuración y no se realizará ninguna prueba de sonido. La tarjeta de sonido quedará completamente configurada. Con la 'Configuración normal' tiene la oportunidad de regular la salida y el volumen, así como de realizar una prueba de sonido. La 'Configuración avanzada' le permite ajustar las opciones del módulo de sonido manualmente.

En este diálogo también puede configurar el joystick pulsando en la casilla del mismo nombre. Seleccione el tipo de joystick en el diálogo que se abre a continuación y pulse después en 'Siguiente'.

Volumen de la tarjeta de sonido

En esta pantalla podrá probar la configuración de la tarjeta de sonido. Use los botones '+' y '–' para regular el volumen. Le recomendamos que lo inicie con un 10 % para no causar daños a sus oídos o al equipo. Tras pulsar el botón 'Probar', debería oírse una prueba de sonido. Si no es así, aumente el volumen. Con 'Siguiente', la configuración del sonido finaliza y el nivel de volumen es almacenado.

Configuración del sonido

Con la opción 'Eliminar', puede eliminar una tarjeta de sonido. Las entradas existentes para las tarjetas de sonido configuradas serán desactivadas en el archivo `/etc/modprobe.d/sound`. Pulsando en 'Opciones' se abre un diálogo en el que puede ajustar las opciones del módulo de sonido manualmente. En el menú 'Añadir tarjeta de sonido' podrá configurar tarjetas de sonido adicionales. Si YaST detecta otras tarjetas de sonido, le dirigirá automáticamente al menú 'Configurar una tarjeta de sonido'. Si YaST no detecta ninguna tarjeta de sonido, irá automáticamente al menú 'Selección manual de la tarjeta de sonido'.

Si dispone de una `Creative Soundblaster Live` o `AWE`, podrá copiar automáticamente las fuentes de sonido CD ROM SF2 al disco duro desde el controlador original de Soundblaster mediante la opción 'Instalar fuentes de sonido'. Estas son grabadas en el directorio `/usr/share/sfbank/creative/`.

Para reproducir archivos Midi deberá tener activada la opción 'Iniciar secuenciador'. De esta manera los módulos necesarios serán cargados junto con los módulos de sonido.

El volumen y la configuración de todas las tarjetas de sonido instaladas se guardan al pulsar 'Finalizar'. La configuración del mezclador se almacena en el archivo `/etc/asound.conf` y la configuración ALSA se añade al final del archivo `/etc/modprobe.conf`.

2.3.8. Tarjetas de TV y radio

Después de arrancar e iniciar el módulo de YaST, aparecerá el diálogo de las 'Tarjetas de TV y radio'. Si su tarjeta ha sido detectada, se mostrará en la lista superior. En este caso marque la línea con el cursor del ratón y seleccione 'Configurar'. Si la tarjeta no ha sido detectada, configure la tarjeta mediante 'Otra (no detectada)'. El botón 'Configurar' le lleva a la selección manual, donde puede escoger su tarjeta en la lista de modelos y fabricantes.

Si ya ha configurado alguna tarjeta de TV o radio, puede editar las configuraciones existentes con 'Cambiar'. En el diálogo 'Resumen de tarjetas de TV y de radio' puede ver todas las tarjetas ya configuradas. Seleccione una tarjeta e inicie la configuración manual con 'Editar'.

Durante la detección automática de hardware, YaST intenta asignar el sintonizador adecuado para la tarjeta. Si no está seguro, escoja 'Predeterminado (detectado)' y compruebe si funciona. Si no ha podido sintonizar todos los canales, puede

deberse a que la detección automática de sintonizadores haya fallado. En este caso pulse 'Escoja sintonizador' y marque el tipo adecuado de sintonizador en la lista de selección.

Si está familiarizado con las especificaciones técnicas, el diálogo de expertos le permite efectuar una configuración más avanzada. Aquí puede seleccionar el módulo del kernel que funciona como controlador de la tarjeta y todos sus parámetros. También puede editar los parámetros del controlador de la tarjeta de TV. Para ello, seleccione los parámetros a editar e introduzca los nuevos valores. Confirme estos con 'Aplicar' o recupere los valores originales con 'Restablecer'.

En el diálogo 'Audio de la tarjeta de TV y radio' puede conectar la tarjeta de TV o radio con la tarjeta de sonido instalada. Además de la configuración de las tarjetas debe usar un cable que conecte la salida de la tarjeta de TV o radio con la entrada externa de audio de la tarjeta de sonido. Para ello, la tarjeta de sonido ya debe estar configurada y la entrada externa activada. Si aún no ha configurado la tarjeta de sonido, hágalo en el diálogo correspondiente con 'Configurar tarjeta de sonido' (véase la sección 2.3.7 en la página 59).

Si la tarjeta de TV o de radio dispone de conexión para altavoces, puede conectarlos directamente y no será necesario configurar la tarjeta de sonido. También hay tarjetas de TV sin función de sonido (por ejemplo para cámaras CCD), que por lo tanto no requieren ninguna configuración de audio.

2.4. Dispositivos de red

Para que los dispositivos de red del sistema puedan ser utilizados un servicio, es necesario iniciarlos antes. La detección y configuración de estos dispositivos se realiza en el grupo de módulos 'Dispositivos de red'. La sección ?? en la página ?? contiene una descripción detallada de la configuración de cualquier tipo soportado de interfaces de red con YaST, así como información general sobre las conexiones a redes. La configuración de dispositivos de red para la comunicación inalámbrica se explica en el capítulo **??** en la página ??.

2.5. Servicios de red

Este grupo contiene herramientas para configurar todo tipo de servicios en la red, como por ejemplo la resolución de nombres, la autenticación de usuarios o los servicios de archivos.

2.5.1. Agente de transferencia de mensajes (MTA)

El módulo de configuración le permite configurar sus opciones de correo si utiliza los programas sendmail o postfix, o envía sus mensajes a través del servidor SMTP de su proveedor. Puede bajar el correo a su ordenador mediante SMTP o con el programa fetchmail, en el que también puede introducir los datos de los servidores POP3 o IMAP de su proveedor. De forma alternativa puede configurar sus datos de acceso POP y SMTP en un programa de correo de su elección por ejemplo KMail o Evolution de la forma habitual (para recibir el correo con POP3 y enviarlo con SMTP). En este caso no necesita este módulo.

Si desea configurar el correo con YaST el sistema le preguntará en la primera ventana del diálogo de correo los datos del tipo de conexión deseada para acceder a Internet. Dispone de las siguientes opciones:

'Permanente' Seleccione esta opción si tiene una línea dedicada para Internet. El ordenador estará conectado permanentemente, por lo que no es necesario ningún marcado adicional. Si el sistema se encuentra en una red local con un servidor central de correo para el envío de mensajes, escoja también esta opción para garantizar un acceso permanente a su correo.

'Telefónica' Esta opción de menú es la adecuada para todos los usuarios que tienen un ordenador que no está conectado a ningún red y que se conectan a Internet de vez en cuando.

Sin conexión Si no dispone de ninguna conexión a Internet y no pertenece a ninguna red, no podrá enviar ni recibir correo electrónico.

Además puede activar el antivirus para los mensajes entrantes y salientes con AMaViS. El paquete correspondiente se instalará de forma automática tan pronto como active el filtrado de correo. En el diálogo posterior especifique el servidor saliente de correo (el servidor SMTP de su proveedor) y los parámetros para el correo entrante. Si utiliza una conexión telefónica (dial-up), puede indicar diversos servidores POP o IMAP para recibir correo a través de distintos usuarios. Finalmente y de forma opcional, puede adjudicar nombres alias, configurar el enmascaramiento o masquerading o crear dominios virtuales. Abandone la configuración de correo con 'Finalizar'.

2.5.2. Otros servicios disponibles

YaST incluye muchos otros módulos de red.

Servidor DHCP YaST le permite configurar su propio servidor DHCP en unos pocos pasos. En el capítulo ?? en la página ?? se recoge información general sobre este tema y se explican los pasos de la configuración con YaST.

Servidor DNS Este módulo sirve para configurar el nombre de host y DNS en caso de que no se hubieran definido durante la configuración del dispositivo de red. También puede utilizarse para cambiar el nombre del ordenador y del dominio. Si ha configurado correctamente el proveedor para DSL, módem o acceso RDSI, verá en la lista las entradas del servidor de nombres. Si se encuentra en una red local, lo más probable es que reciba su nombre de host por medio de DHCP. En ese caso no modifique el nombre.

Servidor HTTP Si desea un servidor web propio puede configurar Apache con ayuda de YaST. Para obtener información adicional sobre este tema, consulte el capítulo **??** en la página ??.

Nombres de host Durante el arranque y en redes pequeñas también es posible realizar la resolución de nombres de host en este módulo en lugar de en DNS. Las entradas de este módulo coinciden con el contenido del archivo `/etc/hosts`. Puede obtener información adicional en la sección /etc/hosts en la página ??.

Cliente LDAP Como alternativa a NIS, la autenticación de usuarios en la red puede llevarse a cabo a través de LDAP. Encontrará información general sobre LDAP así como una descripción detallada de la configuración de un cliente LDAP con YaST en el capítulo **??** en la página ??.

Cliente y servidor NFS NFS le ofrece la posibilidad de trabajar en Linux con un servidor de archivos al que puedan acceder los demás usuarios de la red. En este servidor de archivos puede por ejemplo poner a disposición de los usuarios determinados programas y archivos o también espacio de memoria. En el módulo 'Servidor NFS' puede definir que su ordenador haga las veces de servidor NFS y fijar los directorios a exportar, es decir, los directorios que los usuarios de la red pueden usar. Los usuarios autorizados pueden montar estos directorios en su propia estructura de archivos. Puede obtener información adicional sobre este módulo de YaST y sobre NFS en general en el capítulo **??** en la página ??.

Cliente y servidor NIS Cuando se administran varios sistemas, la gestión local de usuarios (por medio de los archivos `/etc/passwd` y `/etc/shadow`) puede llegar a ser muy laboriosa y poco manejable. En estos casos conviene administrar los datos de usuario de forma centralizada en un servidor

y distribuirlos desde allí a los clientes. Además de LDAP y Samba, puede utilizar NIS para este propósito. Consulte el capítulo ?? en la página ?? para obtener información detallada sobre NIS y su configuración con YaST.

Cliente NTP NTP (Network Time Protocol) es un protocolo para sincronizar el reloj de los ordenadores a través de una red. Puede obtener información adicional sobre NTP en el capítulo **??** en la página ??.

Servicios de red (inetd) Con esta herramienta puede configurar qué servicios de la red, por ejemplo finger, talk, ftp, etc., deben iniciarse al arrancar SUSE LINUX. Estos servicios permiten a usuarios remotos la conexión a su ordenador. Para cada servicio puede fijar unos parámetros distintos. De forma estándar, el servicio que administra el resto de servicios de la red (inetd o xinetd) no se iniciará.

Tras iniciar este módulo, seleccione cuál de los dos servicios quiere iniciar. El daemon seleccionado se puede arrancar con una selección estándar de servicios de red o combinando una selección personalizada de dichos servicios, en la que puede 'añadir', 'borrar' o 'editar' servicios.

Aviso

Configuración de los servicios de red (inetd)

La agrupación y clasificación de los servicios de red en el sistema es un proceso muy complejo que requiere un profundo conocimiento del concepto en el que se basan los servicios de red en Linux.

Aviso

Proxy Este módulo le permite editar la configuración de los proxies para todo el sistema. Puede obtener información detallada sobre los proxies en el capítulo **??** en la página ??.

Administración desde un ordenador remoto
Si desea administrar el sistema desde una máquina remota a través de una conexión VNC, puede autorizar el establecimiento de la conexión con este módulo de YaST. Consulte la sección 3.2.2 en la página 93.

Routing Necesitará esta herramienta si está conectado a Internet por medio de una pasarela a la red local. En el caso de DSL, los datos de la pasarela sólo son relevantes parar la configuración de las tarjetas de red. Los datos introducidos para DSL son datos falsos (dummies) sin ninguna función.

Configuración de un servidor/cliente Samba

Samba se ocupa de regular la comunicación entre máquinas Linux y Windows en redes heterogéneas. Para obtener información adicional tanto sobre Samba como sobre su configuración de cliente y servidor, consulte el capítulo **??** en la página ??.

2.6. Seguridad y usuarios

Una característica básica de Linux es que se trata de un sistema multiusuario. Es decir, distintos usuarios pueden trabajar de manera independiente en el mismo sistema Linux. Cada usuario tiene una cuenta de usuario que consiste de un nombre de usuario y una contraseña personal para entrar en el sistema. Cada usuario tiene su propio directorio personal con sus propios archivos y configuraciones cargadas.

2.6.1. Administración de usuarios

Después de especificar que desea editar usuarios, YaST le ofrece una lista de todos los usuarios locales que tienen acceso al sistema. Si se encuentra en una gran red, puede listar todos los usuarios del sistema (por ejemplo `root`) o usuarios NIS mediante 'Crear filtro'. Existe la posibilidad de crear filtros personalizados. Para añadir usuarios, rellene los campos necesarios en la siguiente máscara. Después los nuevos usuarios se podrán registrar en el ordenador con su nombre de login y la contraseña. En 'Editar', la opción 'Detalles' guarda las opciones más detalladas del perfil de usuario. Es posible configurar la shell de login y el directorio de usuario manualmente. Además es posible asignar el usuario a determinados grupos. El tiempo de validez de la contraseña se configura en 'Configuración de la contraseña'. Todos los parámetros se pueden modificar con el botón 'Editar'. Para eliminar un usuario, selecciónelo en la lista y pulse el botón 'Borrar'.

En la administración avanzada de red tiene la posibilidad de especificar las opciones predeterminadas para crear nuevos usuarios en 'Experto'. Allí también puede seleccionar el tipo de autenticación y la administración de usuarios (NIS, LAN, Samba o Kerberos), así como el algoritmo para codificar la contraseña. Estas opciones de configuración están pensadas para redes de grandes dimensiones.

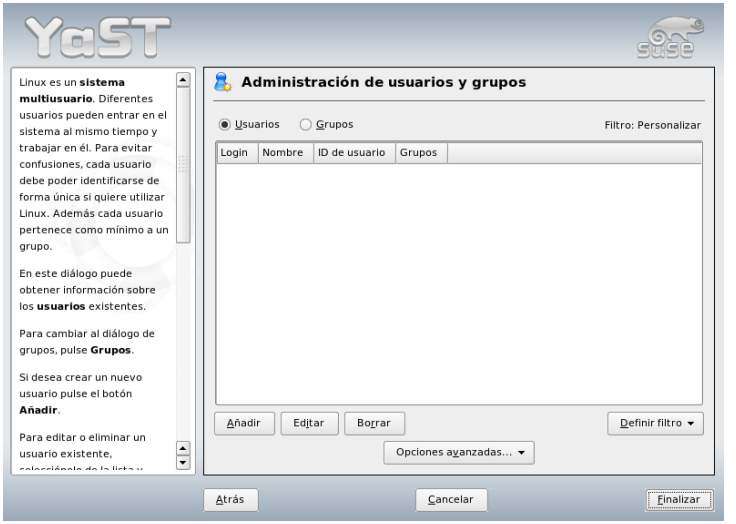

Figura 2.7: *Administración de usuarios*

2.6.2. Administración de grupos

Arranque el módulo de gestión de usuarios del centro de control de YaST o pulse dentro de la gestión de usuarios sobre la casilla 'Grupos'. La funcionalidad de ambas máscaras es idéntica con la diferencia de que aquí se crean grupos en lugar de usuarios.

YaST le ofrece un listado de todos los grupos. Si un grupo debe ser eliminado simplemente selecciónelo de la lista de forma que la línea aparezca en azul oscuro y pulse en 'Eliminar'. En 'Añadir' y 'Editar' indique el nombre, el identificador de grupo (gid) y los miembros del grupo en la correspondiente ventana de YaST De forma opcional, puede adjudicar una contraseña para cambiar a este grupo. La configuración del filtro es idéntica a la del diálogo 'Administración de usuarios'.

2.6.3. Configuración de seguridad

En la pantalla de inicio 'Configuración de seguridad local', a la que puede acceder desde 'Seguridad y usuarios', existen cuatro opciones disponibles: el 'nivel 1'

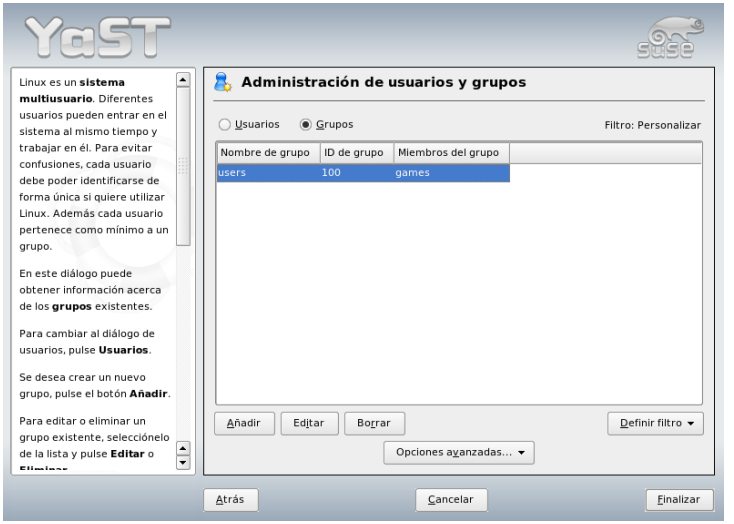

Figura 2.8: *Administración de grupos*

es para una estación de trabajo (preconfigurado), el 'nivel 2' para estaciones de trabajo en red (preconfigurado), el 'nivel 3' para servidores en red (preconfigurado) y la opción 'Configuración personalizada'.

Si selecciona cualquiera de las tres primeras opciones, podrá adoptar una configuración preconfigurada de la seguridad del sistema. Para hacerlo, pulse simplemente sobre 'Finalizar'. La opción 'Detalles' le proporciona acceso a las distintas configuraciones que puede cambiar cuando desee. Si elige 'Configuración personalizada', puede pasar de un diálogo a otro pulsando 'Siguiente'. Aquí hallará los valores preconfigurados en la instalación.

'Configuración de contraseña' Si desea que el sistema compruebe las contraseñas nuevas antes de aceptarlas, seleccione las casillas 'Comprobar nuevas contraseñas' y 'Comprobar plausibilidad de contraseñas'. Especifique la longitud máxima y mínima de la contraseña, además del período de validez de dicha contraseña, y determine con cuántos días de antelación se debe notificar al usuario la expiración de la contraseña cada vez que se registra en la consola de texto.

'Configuración de arranque' Aquí puede especificar cómo debe interpretarse la

combinación de teclas Ctrl-Alt-Del seleccionando la acción deseada. Normalmente, al introducir esta combinación en la consola de texto el sistema se reinicia. Conviene dejar esto tal y como está a no ser que su máquina o servidor sean accesibles para todo el mundo y tema que esta acción se lleve a cabo sin su autorización. Al seleccionar 'Parar' esta combinación provoca el cierre del sistema, con 'Ignorar' no se realiza ninguna acción.

Definir el 'Comportamiento de apagado de KDM' determinando quién tiene permiso para cerrar el sistema de KDM (KDE Display Manager – el login gráfico). Las opciones disponibles son 'Sólo root' (el administrador del sistema), 'Todos los usuarios', 'Nadie' o 'Usuarios locales'. Si selecciona 'Nadie', el sistema solamente puede ser reiniciado desde la consola de texto.

'Configuración del inicio de sesión' Normalmente, después de un intento fallido de login, existe un período de espera antes de que sea posible volver a iniciar la sesión. El propósito de esto es dificultar la entrada al sistema mediante rastreadores de contraseñas (sniffers). Aquí puede activar las opciones 'Registrar los inicios de sesión fallidos' y 'Registrar los inicios de sesión correctos'. Si sospecha que alguien está intentando averiguar su contraseña, puede comprobar las entradas realizadas al sistema a través de los archivos de registro ubicados en `/var/log`. Con la opción 'Permitir inicio de sesión gráfico remoto', otros usuarios podrán acceder a la pantalla de login gráfica a través de la red. Pero esta posibilidad de acceso representa un riesgo potencial para su seguridad, por lo que por defecto se encuentra desactivada.

'Configuración de adduser' Cada usuario posee un número de identificación de usuario así como un nombre alfanumérico. La relación entre ambos se establece mediante el archivo `/etc/passwd` y debería ser unívoca en la medida de lo posible. Con los datos de esta ventana puede definir el rango numérico asignado a la parte numérica del identificador de usuario cuando añade un nuevo usuario. Para los usuarios se recomienda un mínimo de 500. Los números generados automáticamente empiezan a partir de 1000. La configuración de ID de grupo se realiza de la misma forma.

'Configuración adicional' Existen tres opciones diferentes para la 'Configuración de los permisos de archivos': 'Easy', 'Secure' y 'Paranoid'. La primera será suficiente para la gran mayoría de usuarios. El texto de ayuda de YaST le proporcionará información sobre estos tres niveles de seguridad. La opción 'Paranoid' es extremadamente restrictiva y debería ser el punto de partida de algunas configuraciones para un administrador. Si elige 'Paranoid', al administrar aplicaciones individuales deberá contar con molestias

o funciones que faltan, puesto que no tendrá los permisos correspondientes para acceder a diversos archivos.También en esta ventana puede definir qué usuarios pueden iniciar `updatedb`. Este programa se ejecutará automáticamente una vez al día o después de cada arranque y genera una base de datos (locatedb) en la que está almacenada la localización exacta de cada archivo de su ordenador. Si selecciona 'Nadie' (nobody), los usuarios sólo podrá hallar la localización de un archivo en la base de datos para conseguir su ruta (como cualquier otro usuario sin privilegios). Si selecciona `root`, como superusuario podrá crear una lista de todos los directorios con el comando locate. Por último, asegúrese de que la opción 'Incluir directorio actual en la ruta de root' está desactivada (estado predeterminado).

Pulse 'Finalizar' para cerrar la configuración de seguridad.

Figura 2.9: *Configuración de seguridad*

2.6.4. Cortafuegos

Este módulo le permite configurar SuSEfirewall2, para proteger su sistema de los intrusos procedentes de Internet. Puede obtener información detallada sobre el

funcionamiento de SuSEfirewall2 en la sección **??** en la página ??.

Sugerencia

Activación automática del cortafuegos

YaST inicia automáticamente un cortafuegos con una configuración adecuada en todas las interfaces de red configuradas. Por lo tanto, este módulo sólo debe activarse en caso de que desee modificar la configuración estándar del cortafuegos y personalizarla o bien desactivarla por completo.

Sugerencia

2.7. Sistema

2.7.1. Copia de seguridad de las áreas del sistema

El módulo de copias de seguridad de YaST permite realizar fácilmente copias de seguridad del sistema. El módulo no realiza una copia de seguridad completa del sistema, sino que sólo guarda información sobre paquetes que se hayan modificado, áreas críticas del sistema y archivos de configuración.

La configuración de este módulo permite determinar el alcance de la copia. Por defecto se guarda información sobre los paquetes que se hayan modificado desde la última instalación. Aparte de esto se puede guardar mucha información que no pertenece a ningún paquete como por ejemplo muchos archivos de configuración del directorio `/etc` o de su directorio `home`. Adicionalmente es posible archivar también información crítica como la tabla de partición o el MBR. Esta información se utilizará en caso de una recuperación del sistema.

2.7.2. Recuperación del sistema

Con el módulo de recuperación (figura 2.10 en la página siguiente) puede recuperar su sistema a partir de un archivo de copias de seguridad. Siga las instrucciones en YaST. Al pulsar 'Siguiente' aparecerán los distintos diálogos. Al principio introduzca dónde se encuentra cada archivo, ya sea en medios de intercambio, en discos locales o en sistemas de archivos en la red. A continuación, obtendrá las correspondientes descripciones y contenidos del archivo y podrá elegir qué debe ser recuperado.

Además existen dos diálogos adicionales en los que puede escoger los paquetes que han sido añadido nuevos desde la última copia de seguridad y que puede ahora desinstalar así como los paquetes eliminados desde la última copia de seguridad y que ahora puede volver a instalar. Con estos dos pasos adicionales puede restaurar exactamente el estado del sistema tal y como estaba en el momento en que se efectuó la última copia de seguridad.

Aviso

Recuperación del sistema

Puesto que en casos normales este módulo permite instalar, sustituir o desinstalar muchos paquetes y archivos, sólo debería utilizarlo si está familiarizado con las copias de seguridad (backups); de lo contrario, existe el riesgo de perder datos.

Aviso

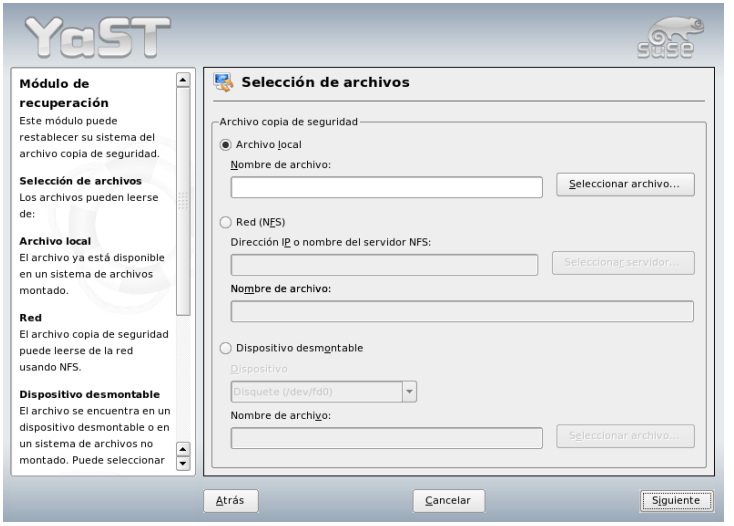

Figura 2.10: *Ventana de inicio del módulo de recuperación*

2.7.3. Creación de disquetes de arranque y rescate

Con este módulo de YaST puede crear disquetes de arranque o rescate con mucha facilidad. Estos disquetes resultan muy útiles si la configuración de arranque del sistema está dañada. El disquete de rescate es especialmente necesario si el sistema de archivos de la partición root está dañado.

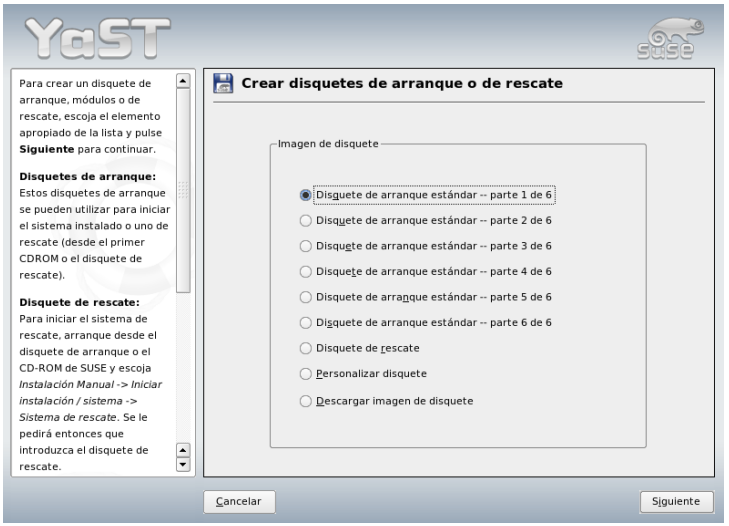

Figura 2.11: *Creación de disquetes de arranque y de rescate*

Las siguientes opciones están disponibles:

'Disquete de arranque estándar' Con esta opción puede crear disquetes de arranque estándar para arrancar un sistema ya instalado. El número de disquetes de arranque depende de la arquitectura. Debe crear todos los disquetes de arranque que aparezcan en el diálogo porque todos ellos son necesarios para iniciar el sistema. También son necesarios para arrancar el sistema de rescate.

'Disquete de rescate' Este disquete contiene un entorno especial que le permite efectuar trabajos de reparación en un sistema ya instalado, por ejemplo comprobar los sistemas de archivos y actualizar el gestor de arranque. Para iniciar el sistema de rescate, arranque primero con los disquetes

de arranque estándar y seleccione 'Instalación manual' → 'Iniciar instalación/sistema' → 'Sistema de rescate'. A continuación se le pedirá que introduzca el disquete de rescate.

'Disquete personalizado' Esta opción sirve para copiar cualquier imagen para un disquete del disco al disquete. Esta imagen ya debe existir en el disco duro.

'Descargar imagen de disquete' Esta opción sirve para descargar una imagen de disquete desde Internet, después de haber introducido el URL y los datos de autenticación para acceder al servidor en Internet.

Para crear los discos, seleccione la opción correspondiente y pulse en 'Siguiente', tras lo cual se le pedirá que introduzca un disquete. Vuelva a pulsar en 'Siguiente', y el contenido se grabará en el disquete.

2.7.4. LVM

El gestor de volúmenes lógicos o Logical Volume Manager (LVM) es una herramienta que le permite particionar el disco duro mediante unidades lógicas. Puede obtener información adicional sobre LVM en la sección 3.6 en la página 100.

2.7.5. Particionamiento

En el diálogo de expertos (figura 2.12 en la página siguiente) puede modificar manualmente el particionamiento de uno o varios discos duros así como añadir, eliminar o editar particiones. Este módulo de YaST también le permite acceder a la configuración de soft RAID y LVM.

Aviso

Si bien es posible modificar las particiones en el sistema instalado, se recomienda que esta tarea sólo sea realizada por expertos. En caso contrario, existe un riesgo muy elevado de pérdida de datos si comete algún error. Cuando vuelva a particionar un disco duro en uso, debe reiniciar el sistema inmediatamente. Resulta más seguro utilizar el sistema de rescate que reparticionar el sistema mientras está en funcionamiento.

Aviso

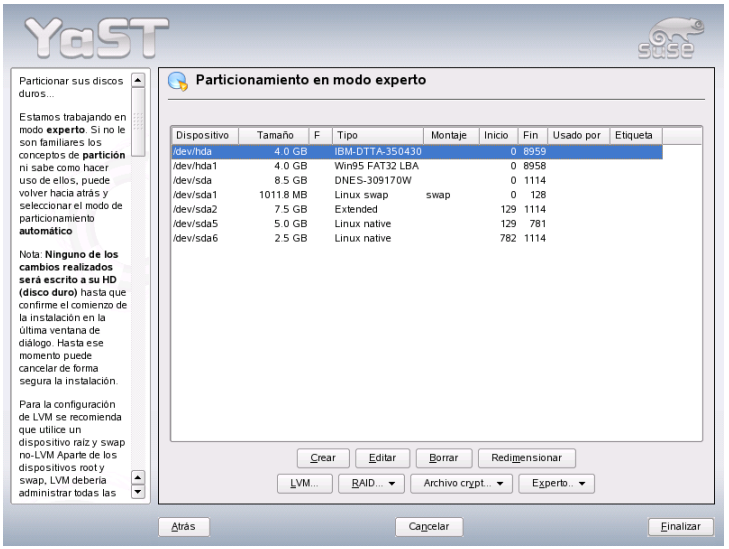

Figura 2.12: *El particionador de YaST en modo experto*

La lista del diálogo experto muestra todos los discos duros y todas las particiones (ya sean existentes o propuestas). Los discos duros se visualizan como dispositivos sin números (por ejemplo `/dev/hda` o `/dev/sda`) mientras que las distintas particiones se representan como partes de estos dispositivos (por ejemplo `/dev/hda1` o `/dev/sda1`). También se muestra el tamaño, tipo, sistema de archivos y punto de montaje de todos los discos duros y particiones. El punto de montaje determina el directorio que se usa para integrar una partición en el árbol de archivos de Linux.

Si ejecuta el diálogo experto durante la instalación, se muestra también el espacio libre del disco duro y se selecciona de forma automática. Si quiere disponer de más espacio para SUSE LINUX, puede liberarlo seleccionando en la lista las particiones del disco duro de abajo a arriba. Así por ejemplo, no es posible escoger la segunda de tres particiones para SUSE LINUX y dejar la primera y tercera para otro sistema operativo.

Crear una partición

Seleccione 'Crear'. Si existen varios discos duros conectados, a continuación aparecerá una ventana de diálogo en la que puede seleccionar un disco duro para la nueva partición. Después debe especificar el tipo de partición (primaria o extendida); puede crear hasta cuatro particiones primarias o tres primarias y una extendida. En la partición extendida en cambio puede crear varias particiones lógicas (ver sección Tipos de particiones en la página 11).

Elija ahora el sistema de archivos que desea utilizar y, en caso necesario, un punto de montaje. YaST sugiere un punto de montaje para cada partición creada. En el apartado siguiente se tratan los distintos parámetros de particionamiento. Después de seleccionar 'Aceptar' para aplicar los cambios, la nueva partición aparecerá en la tabla de particiones. Pulsando 'Siguiente' se aplican los valores actuales y se vuelve a la ventana de diálogo con la propuesta de instalación.

Parámetros de particionamiento

Al crear una nueva partición o modificar una partición ya existente se pueden definir distintos parámetros. En el caso de las nuevas particiones, YaST se encarga de fijar estos parámetros que, por lo general, no deben modificarse. Para configurar los parámetros manualmente, proceda como se describe a continuación:

1. Seleccione la partición.
2. Pulse 'Modificar' para editar la partición y defina los siguientes parámetros:

   ID del sistema de archivos Incluso aunque no desee formatear la partición, indique aquí al menos el identificador del sistema de archivos para que la partición sea registrada correctamente. Los valores posibles son: 'Linux' 'Linux swap', 'Linux LVM', y 'Linux RAID'. Puede encontrar más información sobre LVM y RAID en la sección 3.6 en la página 100 y sección **??** en la página ??.

   Sistema de archivos Si quiere formatear la partición durante la instalación, puede indicar aquí el sistema de archivos que debe tener la partición. Posibles valores son: 'Swap', 'Ext2', 'Ext3', 'ReiserFS' y 'JFS'. Para obtener más información sobre los diversos sistemas de archivos, consulte el capítulo **??** en la página ??.

   Swap es un formato especial que convierte la partición en memoria virtual. Como sistema de archivos estándar para las particiones se usa ReiserFS. Se trata de un sistema de archivos journaling al igual que JFS

y Ext3. Un sistema de archivos de estas características restablece su sistema muy rápidamente en caso de un fallo porque se lleva un registro de los procesos de escritura mientras el sistema está en funcionamiento. Además, ReiserFS resulta muy eficaz manejando grandes cantidades de archivos pequeños. Aunque Ext2 no es un sistema de archivos transaccional (journaling), es muy estable y apropiado para particiones pequeñas, ya que necesita poco espacio del disco duro para su propia gestión.

Opciones del sistema de archivos Aquí puede configurar diversos parámetros del sistema de archivos escogido. Según el sistema de archivos utilizado, se ofrecerán unas u otras posibilidades de configuración para expertos.

Sistema de archivos codificado Si activa la criptografía, todos los datos del disco duro serán codificados. Esto aumenta el nivel de seguridad de los datos pero ralentiza el sistema puesto que la codificación requiere tiempo. Puede obtener información adicional sobre la codificación de sistemas de archivos en la sección **??** en la página ??.

Opciones fstab Aquí puede indicar distintos parámetros para el archivo de administración del sistema de archivos (`/etc/fstab`).

Punto de montaje Indica el directorio del árbol del sistema de archivos en el que se debe montar la partición. Puede seleccionar entre las diversas sugerencias de YaST o bien asignar un nombre arbitrario.

3. Pulse 'Siguiente' para activar la partición.

Si realiza las particiones de forma manual, debe crear una partición swap de al menos 256 MB. Esta partición sirve para almacenar temporalmente los datos de la memoria principal que no sean necesarios en ese momento, a fin de dejar libre la memoria de trabajo para datos más importantes y utilizados con más frecuencia.

Opciones avanzadas

A través de la opción 'Experto' se accede a un menú que contiene los siguientes comandos:

Releer la tabla de particiones Vuelve a cargar el particionamiento del disco. Esta opción puede ser necesaria, por ejemplo, después de particionar manualmente en la consola de texto.

Borrar tabla de particiones y etiqueta de disco

Esta opción reescribe completamente la antigua tabla de particiones, lo que puede resultar útil, por ejemplo, si se tienen problemas con etiquetas de disco no convencionales. Esta acción borra todos los datos del disco duro.

Información adicional sobre particiones

Si utiliza YaST para particionar y este detecta otras particiones en el sistema, dichas particiones se introducen también en el archivo `/etc/fstab` , para facilitar el acceso a estos datos. En este archivo se encuentran todas las particiones existentes en el sistema junto con sus propiedades, como por ejemplo sistema de archivos, puntos de montaje y permisos de usuario.

Ejemplo 2.1: */etc/fstab: particiones_datos*

```
/dev/sda1    /data1    auto      noauto,user 0 0
/dev/sda5    /data2    auto      noauto,user 0 0
/dev/sda6    /data3    auto      noauto,user 0 0
```

Las particiones, ya sean de Linux o del sistema FAT, se pueden introducir con las opciones `noauto` y `user`, con lo que se permite a cualquier usuario montar o desmontar estas particiones. Por motivos de seguridad YaST no utiliza aquí la opción `exec`. Si quiere ejecutar programas o scripts desde allí, añada esta opción manualmente. Esta opción es necesaria si recibe mensajes como `bad interpreter` o `Permission denied`.

LVM y el particionamiento

A través de la opción 'LVM' es posible acceder a la configuración de LVM desde el particionador experto (ver la sección 3.6 en la página 100). No obstante, si en el sistema ya existe una configuración LVM en funcionamiento, ésta se activará automáticamente tan pronto como entre en la configuración LVM por primera vez en una sesión. En este caso no es posible reparticionar un disco que contenga una partición perteneciente a un grupo de volúmenes activado. El motivo es que el kernel de Linux no puede volver a leer la tabla de particiones modificada de un disco duro cuando una partición de ese disco duro está en uso. Sin embargo, si ya dispone de una configuración LVM operativa en el sistema, un reparticionamiento físico no será necesario puesto que bastará con modificar la configuración de los volúmenes lógicos.

Al principio de los volúmenes físicos (PV o "physical volume") se escribe información sobre el volumen en la partición. De este modo, un PV "sabe" a qué grupo de volúmenes (VG) pertenece. Si desea reutilizar una partición de este tipo para otros fines no relacionados con los volúmenes lógicos, se recomienda borrar el principio de ese volumen. Por ejemplo, para el VG `system` y PV `/dev/sda2`, esto puede realizarse con el comando `dd if=/dev/zero of=/dev/sda2 bs=512 count=1`.

Aviso

Sistema de archivos para el arranque

El sistema de archivos utilizado para arrancar (el sistema de archivos raíz o `/boot`) no debe almacenarse en un volumen lógico LVM sino en una partición física normal.

Aviso

2.7.6. Administrador de perfiles (SCPM)

Con el módulo de administración de perfiles (System Configuration Profile Management SCPM) se puede crear y administrar configuraciones individuales completas del sistema y cambiar entre ellas. Esto suele ser muy útil en el caso de ordenadores portátiles, ya que suelen ser utilizadas por distintas personas en distintos lugares (con distintas redes). Pero también de esta forma los equipos fijos pueden poner en funcionamiento distinto hardware o distintas configuraciones de prueba. Si desea más información sobre los fundamentos básicos o el funcionamiento de SCPM, lea la sección correspondiente en el capítulo **??** en la página ??.

2.7.7. Servicios del sistema (niveles de ejecución)

Puede trabajar con SUSE LINUX en distintos niveles de ejecución (runlevel). De forma estándar el sistema se inicia en el nivel 5. Esto significa que es un sistema multiusuario, que tiene acceso a redes y una interfaz gráfica (sistema X Windows). Otros niveles son: sistema multiusuario con redes pero sin X (nivel 3), sistema multiusuario sin redes (nivel 2), sistema de un único usuario (niveles 1 y S), apagar el sistema (nivel 0) y reiniciar el sistema (nivel 6).

Sobre todo, los distintos niveles de ejecución son útiles cuando los niveles más altos tienen problemas con los distintos servicios (X o redes). Entonces se puede

iniciar el sistema en un nivel de ejecución más bajo y reparar el servicio correspondiente. Además muchos servidores funcionan normalmente sin interfaz gráfica, por lo que se deben iniciar por ejemplo en el nivel 3.

Por lo general, los usuarios normales sólo necesitan el nivel estándar (5). Si por ejemplo la interfaz gráfica de su máquina se queda colgada, puede desactivar el sistema X Windows al iniciar el ordenador introduciendo la combinación de teclas Ctrl-Alt-F1 en una consola, entrar como root y pasar al nivel 3 con el comando `init 3`. De esta forma se cerrará el sistema X Windows. Para volver a arrancar, hágalo simplemente con `init 5`.

Puede obtener información adicional sobre los niveles de ejecución en SUSE LINUX así como una descripción del editor de niveles de ejecución de YaST en el capítulo **??** en la página ??.

2.7.8. Editor para sysconfig

En el directorio `/etc/sysconfig` se encuentran los archivos con las configuraciones más importantes para SUSE LINUX. El editor de sysconfig presenta todas las posibilidades de configuración. Se puede modificar los valores que después quedarán guardadas en los distintos archivos de configuración. La edición manual no suele ser necesaria, ya que los archivos se ajustan automáticamente al instalar nuevos paquetes o al configurar distintos servicios. Puede obtener información adicional sobre `/etc/sysconfig` en SUSE LINUX y sobre el editor para sysconfig de YaST en el capítulo ?? en la página ??.

2.7.9. Selección de la zona horaria

Aunque la zona horaria ya se define durante el proceso de instalación, aquí podrá realizar modificaciones. Simplemente pulse en su país y seleccione 'Hora local' o 'UTC' (Universal Time Coordinated). 'UTC' es muy usado en sistemas Linux. Las máquinas con otros sistemas operativos como Microsoft Windows usan hora local.

2.7.10. Selección del idioma

El idioma seleccionado puede cambiarse en cualquier momento. La configuración del idioma es global, es decir, vale tanto para YaST como para el escritorio.

2.8. Otros

2.8.1. Enviar una petición de soporte

El precio de compra de SUSE LINUX incluye asistencia técnica para la instalación. Puede encontrar más información (por ejemplo alcance del soporte, dirección, números de teléfono, etc.) en la página web `http://www.novell.com/linux/suse/`.

YaST le permite enviar directamente por correo electrónico una consulta de soporte al equipo de SUSE. Este servicio sólo está disponible después de haberse registrado. Introduzca la información correspondiente al principio del correo electrónico (el código de registro se encuentra en la carátula del CD). En cuanto a la consulta en sí, seleccione en la ventana la categoría del problema y descríbalo (figura 2.13 en la página siguiente) según se le indica en la ayuda de YaST. En ella se informa de cómo describir el problema de forma óptima para recibir ayuda lo antes posible.

Sugerencia

Si necesita asistencia avanzada (como por ejemplo para problemas más específicos), visite `http://support.novell.com/linux/`.

Sugerencia

2.8.2. Registro de arranque

Los registros de arranque son mensajes que aparecen en pantalla cuando se inicia el sistema. Estos mensajes se encuentran en el archivo `/var/log/boot.msg`. Puede verlos fácilmente con este módulo de YaST y comprobar si todos los servicios y herramientas han arrancado de la forma prevista.

2.8.3. Registro de sistema

Los registros de sistema documentan el funcionamiento del sistema y se almacenan en el archivo `/var/log/messsages`. Los mensajes del kernel aparecen aquí ordenados por fecha y hora.

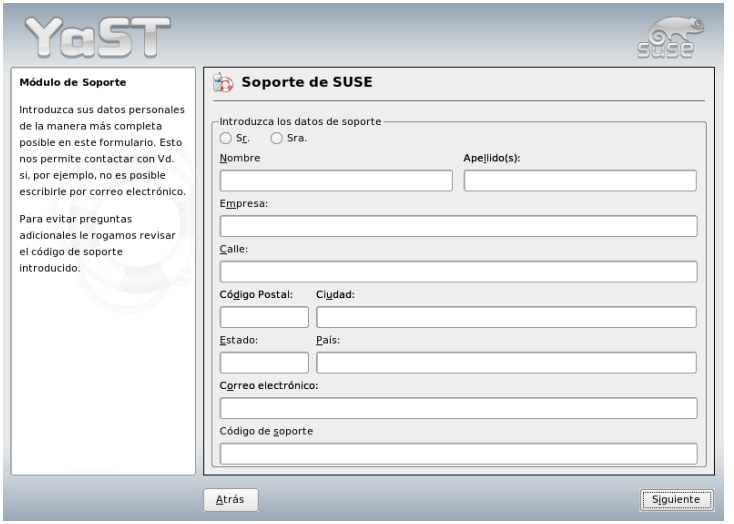

Figura 2.13: *Enviar una consulta de soporte*

2.8.4. Cargar CD de controladores del fabricante

Con este módulo, puede instalar automáticamente controladores de dispositivos desde un CD Linux que contenga controladores para SUSE LINUX. Al realizar una nueva instalación de SUSE LINUX puede cargar los controladores del CD del fabricante con ayuda de este módulo de YaST una vez finalizada la instalación.

2.9. YaST en modo texto (ncurses)

Este apartado 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. El apartado incluye información básica para trabajar con YaST en modo texto (ncurses).

Al arrancar YaST en modo texto, lo primero que aparece es el centro de control de YaST (ver figura 2.14 en la página siguiente). En ella puede observar tres secciones: 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'.

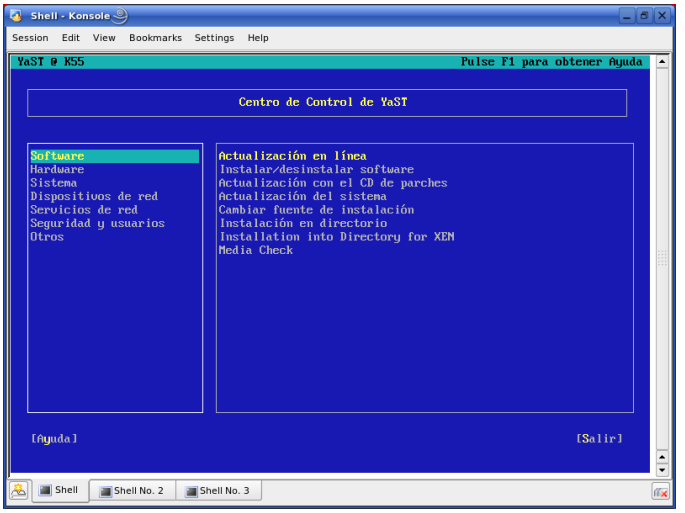

Figura 2.14: *La ventana principal de YaST ncurses*

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).

2.9.1. Navegación en los módulos de YaST

En la siguiente descripción de los elementos de control de los módulos de YaST se parte de la base de que las teclas de función y las combinaciones con (Alt) funcionan y no se utilizan de otro modo en el sistema. Consulte la sección 2.9.2 en la página siguiente para obtener información sobre posibles excepciones.

Navegación entre botones/listas de selección:
Con (Tab) y (Alt)–(Tab) o (Shift)–(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. Si alguna entrada sobresale de un cuadro debido a su anchura, puede navegar horizontalmente de izquierda a derecha con (Shift)–(→) o bien (Shift)–(←) (asimismo puede utilizar la combinación de teclas (Ctrl)–(e) o bien (Ctrl)–(a)). Esta combinación también funciona en aquellas situaciones en las que las teclas (→) o (←) ocasionarían un cambio del cuadro activo o de la lista de selección actual, como es el caso en el centro de control.

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). Al igual que los botones normales, las casillas de control y los botones con paréntesis también pueden activarse directamente por medio de (Alt)–(letra_amarilla). En este caso no es necesario confirmar la selección con (Intro). Por el contrario, cuando se navega con la tecla de tabulación, la ejecución de la acción seleccionada o la activación de una entrada de menú sí deben volver a confirmarse con (Intro).

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 en cada módulo se ofrecen distintos botones (detalles, info, añadir, eliminar...). Por ejemplo, para los amigos del antiguo YaST1, los botones 'OK', 'Siguiente' y 'Terminar' se encuentran en la tecla (F10). La Ayuda de YaST, a la que puede acceder con (F1), le proporciona información sobre las funciones que hay en cada tecla F.

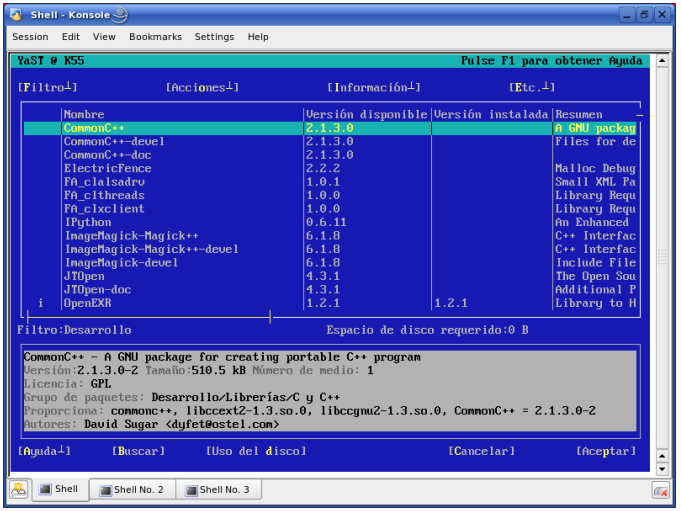

Figura 2.15: *El módulo de instalación de software*

2.9.2. Limitaciones de las combinaciones de teclas

Si en su sistema con un servidor X en funcionamiento es posible utilizar combinaciones de teclas con Alt con efecto en todo el sistema, puede que estas no funcionen en YaST. Además es posible que teclas como Alt o Shift ya estén ocupadas por otras configuraciones del terminal utilizado.

Alt en lugar de Esc Las combinaciones con Alt pueden realizarse utilizando Esc en vez de Alt, por ejemplo Esc–h puede sustituir a Alt–h.

Saltar hacia adelante o hacia atrás con Ctrl–f y Ctrl–b
En caso de que las combinaciones con Alt y Shift ya estén ocupadas por el gestor de ventanas o el terminal, utilice de forma alternativa las combinaciones Ctrl–f (hacia adelante) y Ctrl–b (hacia atrás).

Limitaciones de las teclas de función En SUSE LINUX las teclas F también están ocupadas con funciones. También aquí puede que determinadas teclas de función ya estén ocupadas según el terminal escogido y por lo tanto no estén disponibles para YaST. Sin embargo, en una consola de texto, las com-

binaciones con Alt y las teclas de función deberían estar totalmente disponibles.

2.9.3. Arranque de módulos individuales

Para ahorrar tiempo, los módulos de YaST se pueden iniciar individualmente. Basta con introducir: `yast <nombre_módulo>`.

El módulo de red, por ejemplo, se arranca con `yast lan`. Puede obtener una lista de nombres de todos los módulos disponibles en el sistema con `yast -l` o con `yast --list`.

2.9.4. El módulo YOU

Al igual que cualquier otro módulo de YaST, la actualización en línea de YaST (YOU – YaST Online Update) puede controlarse e iniciarse desde una consola como usuario `root` con el comando:

```
yast online_update .url <url>
```

`yast online_update` activa el módulo correspondiente. De manera opcional puede introducir también `url`. Mediante esta entrada asigna a YOU un servidor (local o remoto) del cual deben obtenerse todos los datos y parches. Si no ha especificado dicha entrada en el comando inicial, puede seleccionar el servidor/directorio más tarde en la máscara de YaST. El botón 'Configurar actualización totalmente automática' le permite configurar un cronjob que actualice el sistema automáticamente.

2.10. Actualización en línea desde la línea de comandos

La herramienta de la línea de comandos online_update le permite actualizar su sistema de forma totalmente automática, por ejemplo a partir de scripts. Un escenario de aplicación concreto: usted desea que, periódicamente y a la misma hora, su sistema busque actualizaciones en un servidor determinado y descargue los parches y la información correspondiente pero sin instalarlos. Posteriormente desea examinar los parches descargados y seleccionar los que han de instalarse:

Para ello, configure un cronjob que ejecute el siguiente comando:

```
online_update -u <URL> -g <parche_tipo>
```

La opción `-u` introduce la URL base del árbol de directorios de la que deben obtenerse los parches. Se soportan los protocolos `http`, `ftp`, `smb`, `nfs`, `cd`, `dvd` y `dir`. Por medio de la opción `-g`, los parches se descargan y guardan en un directorio local sin ser instalados. De manera opcional, puede filtrar los parches en función de su tipo: `security` (actualizaciones que afectan a la seguridad del sistema), `recommended` (actualizaciones cuya instalación se recomienda) y `optional` (actualizaciones optativas). Si no se especifica ningún tipo de parche, online_update descarga todos los parches disponibles de tipo `security` y `recommended`.

A continuación puede instalar inmediatamente los parches descargados sin examinarlos. online_update guarda los parches en la ruta `/var/lib/YaST2/you/mnt`. Para instalarlos, ejecute el comando:

```
online_update -u /var/lib/YaST2/you/mnt/ -i
```

El parámetro `-u` pasa la URL (local) donde se encuentran los parches que van a ser instalados. La opción `-i` inicia el proceso de instalación.

En cambio, para examinar y seleccionar los parches descargados antes de proceder a instalarlos, active la máscara de YOU:

```
yast online_update .url /var/lib/YaST2/you/mnt/
```

A continuación, YOU se inicia y selecciona como fuente de los parches el directorio local que contiene los parches descargados en lugar de un directorio remoto en Internet. Finalmente puede seleccionar los parches deseados por medio del gestor de paquetes como en cualquier otra instalación.

Si YaST Online Update se inicia desde la línea de comandos, es posible utilizar parámetros para controlar su funcionamiento. Para ello, las acciones respectivas se expresan mediante parámetros de línea de comando de este modo: `online_update [parámetro_línea_de_comandos]`. A continuación le presentamos una lista de los parámetros posibles junto con su significado.

`-u URL` URL base del árbol de directorios del que deben descargarse los parches.

`-g` Descargar parches sin instalarlos.

-i Instalar parches ya cargados pero sin descargar parches nuevos.

-k Comprobar si hay nuevos parches disponibles.

-c Mostrar la configuración actual.

-p producto Producto para el que se van a obtener los parches.

-v versión Versión del producto para la que se van a obtener los parches.

-a arquitectura Arquitectura base del producto para la que se van a obtener los parches.

-d Ensayo (”dry run”). Descargar los parches y simular la instalación. El sistema no se modifica. Se utiliza sólo con fines de pruebas.

-n No se comprueba la firma de los archivos descargados.

-s Mostrar lista de parches disponibles.

-V Modo verboso que produce mensajes sobre las actividades del sistema.

-D Modo de depuración para expertos e identificación de fallos.

Para obtener información adicional sobre online_update, vea la salida del comando `online_update -h`.

Variantes específicas de la instalación

SUSE LINUX puede instalarse de forma flexible atendiendo a las necesidades individuales de cada uno. 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 las distintas opciones de instalación, como por ejemplo la instalación en modo texto con YaST o el uso de diferentes medios de instalación (CD-ROM, NFS). En este capítulo se incluyen consejos de cara a problemas en la instalación así como instrucciones para solucionarlos. Al final del capítulo encontrará una sección y un apartado que describe en detalle el proceso de particionamiento.

3.1. linuxrc

Cada ordenador dispone de ciertas rutinas BIOS que se ejecutan después de encenderlo y que se encargan de iniciar el hardware para permitir el arranque. Durante el arranque real, estas rutinas cargan una imagen que es ejecutada por el ordenador y que controlará el proceso de arranque posterior. Esta imagen consiste normalmente en un gestor de arranque que permite al usuario seleccionar un sistema instalado o un sistema de instalación. Cuando se selecciona la instalación de SUSE LINUX se carga una imagen de arranque que contiene un kernel y un programa llamado linuxrc.

linuxrc es un programa que analiza e inicia el sistema como preparación al auténtico proceso de instalación. Normalmente se ejecuta sin interacción del usuario e inicia YaST al finalizar. Si desea transmitir parámetros especiales a un módulo o si la detección automática de hardware falla, puede que necesite ejecutar linuxrc de forma interactiva. Inicie para ello la instalación manual.

linuxrc no sólo sirve para la instalación sino también como herramienta de arranque para un sistema Linux instalado o incluso para arrancar un sistema de rescate autónomo (basado en un ramdisk). Puede obtener información adicional en la sección **??** en la página ??.

Si el sistema utiliza un RAM disk inicial (initrd), un script de shell también llamado linuxrc se encarga de cargar los módulos durante el arranque. Dicho script, generado dinámicamente por el script `/sbin/mkinitrd`, no debe confundirse con el programa linuxrc que se utiliza para la instalación y del cual difiere completamente.

3.1.1. Paso de parámetros a linuxrc

Existe la posibilidad de pasar parámetros a linuxrc que modifiquen el comportamiento de inicio. linuxrc busca un archivo de información que puede encontrarse en un disquete o bien en `initrd` bajo `/info`. Sólo entonces linuxrc lee los parámetros del prompt del kernel. Los valores predeterminados pueden modificarse en el archivo `/linuxrc.config`, que es el primero en ser leído. No obstante, se recomienda introducir los cambios en un archivo de información.

Sugerencia

Para ejecutar linuxrc en modo manual, introduzca el parámetro "manual=1" en el prompt de instalación.

Sugerencia

Un archivo de información está formado por palabras claves y sus valores respectivos y presenta la siguiente estructura: `key: value`. Estos pares compuestos de palabra clave y valor pueden pasarse al kernel en la forma `key=value` en la línea de comandos del arranque. El archivo `/usr/share/doc/packages/linuxrc/linuxrc.html` contiene una lista de todas las posibles palabras clave. Algunas de las más importantes se mencionan a continuación con valores de muestra:

Install: URL (nfs, ftp, hd, ...) Definición de la fuente de instalación mediante `URL`. Los protocolos permitidos son `cd`, `hd`, `nfs`, `smb`, `ftp`, `http` y `tftp`. La sintaxis es como la habitual de los navegadores, por ejemplo:

- `nfs://<Servidor>/<Directorio>`
- `ftp://[Usuario[:Contraseña]@]<Servidor>/<Directorio>`

Netdevice: <eth0> La palabra clave `Netdevice:` especifica la interfaz que debe usar linuxrc en caso de que haya varias interfaces ethernet en el servidor de instalación.

HostIP: <10.10.0.2> Define la dirección IP del ordenador.

Gateway: <10.10.0.128> Si el servidor de instalación no se encuentra dentro de la misma subred del ordenador a instalar, se puede acceder a este a través de la pasarela aquí indicada.

Proxy: <10.10.0.1> En el caso de usar los protocolos ftp o http, se puede configurar el uso de un proxy mediante el parámetro `Proxy:`.

ProxyPort: <3128> Esta es la opción para indicar un puerto del proxy que sea diferente al puerto estándar.

Textmode: <0|1> Es el parámetro para arrancar YaST en modo texto.

VNC: <0|1> Por medio de VNC es posible configurar en modo gráfico ordenadores que no disponen de una consola gráfica. El parámetro VNC activa este servicio en el sistema utilizado para la instalación. Compare con el parámetro `VNCPassword`.

VNCPassword: <contraseña> Define una contraseña para una instalación VNC a fin de controlar el acceso a la sesión.

UseSSH: <0|1> Habilita el acceso a linuxrc vía SSH. Esto permite la instalación con YaST en modo texto.

SSHPassword: <contraseña> Define la contraseña del usuario `root` para acceder a linuxrc.

Insmod: <módulo> <parámetro> Determina un módulo que debe ser cargado por el kernel así como los parámetros necesarios. Dichos parámetros se indican separados por espacios.

AddSwap: <0|3|/dev/hda5> Cualquier valor positivo activa como `swap` la la partición con el número indicado; 0 como valor no activa ninguna. También puede indicar el nombre de la partición.

3.2. Instalación a través de VNC

VNC (*Virtual Network Computing*) es una solución cliente servidor que permite acceder a un servidor X remoto a través de un cliente ligero y de fácil manejo. El cliente está disponible para diversos sistemas operativos como Microsoft Windows, MacOS de Apple y Linux.

El cliente VNC vncviewer garantiza la representación gráfica y el control de YaST durante el proceso de instalación. Antes de arrancar el sistema a instalar, hay que preparar un ordenador remoto de tal forma que pueda acceder a este sistema a través de la red.

3.2.1. Preparativos para la instalación VNC

El kernel necesita algunos parámetros para realizar una instalación vía VNC. Estos parámetros se han de pasar al kernel antes del arranque con las siguientes opciones en la línea de arranque:

```
vnc=1 vncpassword=<xyz> install=<fuente>
```

`vnc=1` significa que el servidor VNC se ejecuta en el sistema de instalación. `vncpassword` define la contraseña que se debe utilizar posteriormente. Se puede indicar la fuente de instalación (`install`) bien manualmente (indicación del protocolo y URL al directorio en cuestión) o bien utilizar la instrucción `slp:/`. Con esta instrucción la fuente de instalación se averigua automáticamente con una consulta SLP. Puede obtener más información sobre SLP en el capítulo **??** en la página ??.

3.2.2. Clientes para la instalación VNC

La conexión al ordenador de instalación y al servidor VNC que allí se ejecuta se establece a través de un cliente VNC. SUSE LINUX utiliza para ello vncviewer, incluido en el paquete `xorg-x11-Xvnc`. Para acceder al servidor VNC desde un sistema Windows, instale el programa tightvnc que se encuentra en el primer CD de SUSE LINUX en el directorio `/dosutils/tightvnc`.

Inicie el cliente VNC elegido e introduzca la dirección del sistema de instalación así como la contraseña de VNC cuando se lo pida el sistema.

Como alternativa también puede establecer conexiones VNC con un navegador con soporte Java. Para realizar tal conexión, introduzca lo siguiente en el apartado de la URL:

```
http://<dirección-IP_sistema_instalación>:5801/
```

Una vez que la conexión se ha establecido, YaST arranca y se inicia la instalación.

3.3. Instalación en modo texto con YaST

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. Los usuarios con discapacidad visual también pueden utilizar el modo texto para realizar la instalación con ayuda de los dispositivos de salida adecuados.

En primer lugar debe definir el orden de arranque en la BIOS del ordenador de tal forma que el sistema se inicie desde la unidad de CD-ROM. Introduzca el DVD o CD1 en la unidad correspondiente y reinicie el ordenador. Al cabo de unos instantes aparece la pantalla de bienvenida.

Tiene 10 segundos para elegir 'Manual Installation' con las teclas ↑ y ↓ para que *no* se arranque automáticamente el sistema instalado. Indique en la línea `Boot Options` los parámetros de arranque que su hardware pudiera requerir. Normalmente no es necesario indicar parámetros especiales. Si selecciona el idioma del teclado como idioma de la instalación, la disposición del teclado se configurará correctamente facilitando así la entrada de parámetros.

La tecla (F2) ('video mode') le permite definir la resolución de pantalla para la instalación. Si la tarjeta gráfica le ocasiona problemas durante la instalación, pulse 'Text mode' para acceder al modo texto. Finalmente pulse (Intro). A continuación aparece una ventana con la indicación de progreso Loading Linux kernel, tras lo que se arranca el kernel y se inicia linuxrc. El programa linuxrc está basado en menús y espera las indicaciones del usuario.

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'. En caso de dificultades con ACPI (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 sobreescribe `acpi=off`.

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

Consulte también los artículos relacionados de la base de datos de soporte a los que puede acceder con la palabra clave "acpi" en `https://portal.suse.com`

Escoja la opción 'Memory Test', para comprobar el estado de la memoria cuando aparezcan problemas inexplicables al cargar el kernel o durante la instalación. Linux plantea grandes exigencias al hardware, por lo que la memoria debe estar configurada correctamente. Puede obtener información adicional en la base de datos de soporte con la palabra clave "memtest86". Se recomienda realizar la prueba de memoria por la noche.

3.4. Consejos y trucos

Algunos equipos carecen de unidad de CD-ROM, aunque sí disponen de una de discos flexibles. En estos casos, a fin de poder realizar la instalación, es necesario crear un disco de arranque para poder iniciar el sistema.

Necesita un disco flexible de 3.5" y alta densidad para crear un disquete de arranque a partir de las imágenes que se suministran. En el directorio `boot` del CD 1 se encuentran varias imágenes (images) de disquetes. Estas imágenes pueden copiarse en disquetes utilizando los programas de ayuda adecuados. Los disquetes pasan a llamarse entonces disquetes de arranque.

Estas imágenes de disquete contienen también el cargador o 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.

3.4.1. Crear disquetes de arranque con rawwritewin

El programa gráfico rawwritewin le permite crear disquetes de arranque en Windows. Encontrará este programa en el CD 1 de Windows en el directorio `dosutils/rawwritewin`.

Una vez iniciado el programa ha de introducir el archivo imagen (image file). Dichas imágenes se encuentran también en el CD 1 en el directorio boot. Como mínimo necesitará introducir las imágenes `bootdisk` y `modules1`. Para ver estas imágenes con el navegador de archivos deberá cambiar el tipo de archivo a `all files`. Después introduzca un disquete en la disquetera y pulse 'Write'.

Para crear otros disquetes a partir de las imágenes (`modules1`, `modules2`, `modules3`, y `modules4`), simplemente repita este procedimiento tantas veces como sea preciso. 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.

3.4.2. Crear disquetes de arranque con rawrite

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

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

1. Introduzca el CD 1 de SUSE LINUX.

2. Abra una ventana de DOS (en el menú Inicio bajo 'Accesorios' → 'Símbolo del sistema').

3. Ejecute el programa rawrite.exe con la ruta correcta del lector de CD. En el siguiente ejemplo, se asume que se encuentra ubicado en el directorio `Windows` del disco duro `C:` y el lector de CD tiene asignada la letra `D:`.

   ```
   d:\dosutils\rawrite\rawrite
   ```

4. Después de arrancar, el programa solicita el tipo de fuente (source) y el destino (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.

   ```
   d:\dosutils\rawrite\rawrite
   RaWrite 1.2 - Write disk file to raw floppy diskette

   Enter source filename: 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 (Ctrl)-(C).

3.4.3. Crear un disquete de arranque bajo un sistema de tipo Unix

Dispone de un sistema Linux o de 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:

   ```
   fdformat /dev/fd0u1440
   ```

   Este comando comprueba también si el disquete está libre de errores. No utilice nunca un disco que contenga errores.

2. Introduzca el CD 1 en la unidad de CD-ROM y cambie al directorio `boot` en el CD: En las versiones actuales de SUSE ya no es necesario montar los CDs.

   ```
   cd /media/cdrom/boot
   ```

3. Generar el disquete de arranque con:

   ```
   dd if=bootdsk1 of=/dev/fd0 bs=8k
   ```

4. Repita el proceso con las imágenes `bootdsk2` y `bootdsk3`.

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.

La creación de un disquete de módulos no es un proceso trivial. Puede encontar una detallada información al respecto en `/usr/share/doc/packages/yast2-installation/vendor.html`.

3.4.4. Arrancar con un disquete (SYSLINUX)

El disquete de arranque puede utilizarse siempre que existan requisitos especiales a la hora de realizar la instalación (por ejemplo unidad de CD-ROM no disponible). 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:

1. Comprobar si la BIOS soporta un framebuffer adecuado para VESA 2.0 y si el kernel puede arrancarse en consecuencia.
2. Evaluar los datos del monitor (información DDC).
3. Se lee el primer bloque del primer disco duro (MBR) para definir posteriormente la asignación de BIOS IDs a los nombres de dispositivos Linux (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.

Sugerencia

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.

Sugerencia

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`.

► **x86**
En sistemas x86 es posible arrancar con el segundo CD además de con el CD 1. Mientras que el CD 1 utiliza 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 fallback). ◄

3.4.5. ¿Soporta Linux mi lector CD-ROM?

Se puede decir que, por lo general, Linux soporta la mayoría de los lectores CD-ROM. Si no logra arrancar desde la unidad de CD-ROM, inténtelo mediante el CD 2.

Si el equipo carece tanto de unidad de CD-ROM como de disquete, existe la posibilidad de arrancar el sistema desde una unidad de CD-ROM externa conectada a través de USB, FireWire o SCSI. Esta opción depende fundamentalmente de si la BIOS soporta el hardware en cuestión, por lo que es posible que necesite actualizar la versión de ésta si experimenta algún problema.

3.4.6. Instalación desde una fuente en la red

En ocasiones no es posible efectuar una instalación estándar a través de un lector de CD-ROM. Por ejemplo, cuando el lector de CD-ROM es un modelo propietario antiguo no soportado, o si no dispone de unidad de CD-ROM en el segundo

ordenador (ej. un portátil) pero sí una tarjeta Ethernet. SUSE LINUX ofrece la posibilidad de instalar el sistema en equipos sin CD-ROM a través de una conexión de red. En estos casos se suele utilizar NFS o FTP vía Ethernet.

La asistencia técnica 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 instalación.
2. Arrancar el sistema que se va a instalar con un disquete, CD o desde la red y configurar la red.

La fuente de instalación puede estar disponible a través de diversos protocolos, como por ejemplo NFS y FTP. Para obtener información sobre la instalación en sí, consulte la sección 3.1.1 en la página 90.

3.5. Dispositivos SCSI y nombres de dispositivo permanentes

Los dispositivos SCSI tales como las particiones del disco duro reciben de forma más o menos dinámica nombres de archivo de dispositivo durante el arranque. Esto no supone ningún problema siempre que no se modifique el número o la configuración del dispositivo. No obstante, si se incorpora al sistema un nuevo disco duro SCSI y el kernel lo detecta antes que al disco duro que ya existía, el antiguo disco duro recibe un nuevo nombre y no concuerda con las entradas de la tabla `/etc/fstab`.

Este problema puede evitarse con el script de arranque del sistema `boot.scsidev`. El script puede activarse por medio del comando `/sbin/insserv` y los parámetros de arranque necesarios se guardan en el archivo `/etc/sysconfig/scsidev`. A continuación, el script `/etc/rc.d/boot.scsidev` define nombres de dispositivo permanentes en el directorio `/dev/scsi/`, que pueden utilizarse en el archivo `/etc/fstab`. Si se debe emplear nombres de dispositivo permanentes, es posible definirlos en el archivo `/etc/scsi.alias`. Vea también el comando `man scsidev`.

En el modo experto del editor de niveles de ejecución, debe activar `boot.scsidev` para la fase `B` a fin de que se creen en `/etc/init.d/boot.d` los enlaces necesarios para que los nombres permanentes sean generados durante el proceso de arranque.

Sugerencia

Nombres de dispositivo y udev

Aunque `boot.scsidev` se sigue soportando en SUSE LINUX, se recomienda utilizar udev en la medida de lo posible para generar nombres de dispositivo permanentes. udev se encarga de realizar las entradas en `/dev/by-id/`.

Sugerencia

3.6. Configuración de LVM

Esta sección describe brevemente los principios en los que se basa LVM así como las características básicas que lo convierten en una útil herramienta con muchas aplicaciones. Consulte la configuración de LVM con YaST en la sección **??** en la página ??.

Aviso

El empleo de LVM puede estar asociado con situaciones de riesgo, tales como pérdida de datos. Los bloqueos de aplicaciones, cortes de alimentación y ejecución de comandos erróneos son también una fuente de riesgo. Le recomendamos que realice una copia de seguridad antes de implementar LVM o reconfigurar los volúmenes. No ejecute nunca estas operaciones si no dispone de una copia de sus datos.

Aviso

3.6.1. El gestor de volúmenes lógicos (LVM)

El gestor de volúmenes lógicos (Logical Volume Manager o 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 a las particiones físicas. Los VG se pueden extender por varios discos, de tal forma que un solo VG puede estar constituido por más de una unidad o partes de ellas. Así, el LVM proporciona un cierto nivel de abstracción en relación al espacio físico del disco que permite que su organización pueda ser modificada de una forma mucho más fácil y segura que un reparticionamiento físico. Puede encontrar información adicional a este respecto en la sección Tipos de particiones en la página 11 y la sección 2.7.5 en la página 73

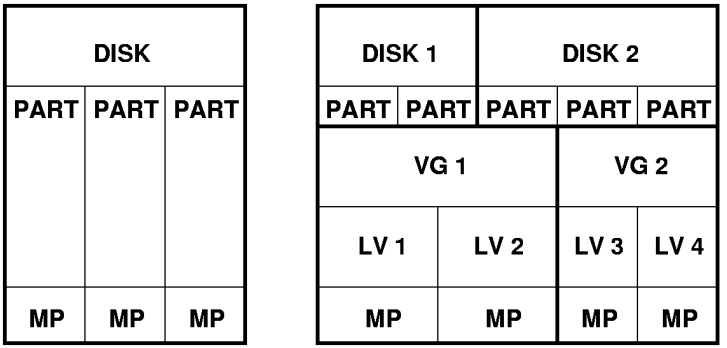

Figura 3.1: *Particionamiento físico frente a LVM*

En la figura **??** en esta página puede encontrar una comparación entre el particionamiento físico (izquierda) y el uso del LVM (derecha). En el lado izquierdo, se ha dividido un solo disco en tres particiones físicas (PART), con un punto de montaje (MP) para cada una, de tal forma que el sistema operativo pueda acceder a ellas. A la derecha, se han dividido dos discos en dos y tres particiones físicas cada uno. Se han definido dos grupos de volúmenes LVM (VG 1 y VG 2).VG 1 contiene dos particiones del disco DISK 1 y una del DISK 2. VG 2 emplea las dos particiones restantes del DISK 2. En LVM, las particiones físicas que son incorporadas a un grupo de volúmenes se denominan volúmenes físicos (Physical volume, PV). Dentro de los grupos de volúmenes se han definido cuatro volúmenes lógicos (desde LV 1 hasta LV 4). Estos volúmenes pueden emplearse por el sistema operativo mediante los puntos de montaje asociados. La línea divisoria entre los diferentes volúmenes lógicos no tiene por qué coincidir con la división de una partición. Por ejemplo, fíjese en el límite entre LV 1 y LV 2 que se muestra en este

ejemplo.

Características de LVM:

- Es posible juntar varias particiones o discos para formar una gran partición lógica.
- Si un LV se queda (por ejemplo `/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 por ejemplo en el caso de bases de datos, archivos de música, 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 "Logical Volume Manager" (LVM) en el HowTo oficial de LVM `http://tldp.org/HOWTO/LVM-HOWTO/`.

Con la versión 2.6 del kernel, LVM se ha actualizado a la versión 2. Esta versión, que es compatible con la versión previa de LVM, puede seguir administrando grupos de volúmenes ya existentes. LVM2 no necesita parches del kernel y utiliza el mapeador de dispositivos (`device mapper`) integrado en el kernel 2.6. A partir de este kernel, LVM sólo puede utilizarse en su versión 2. Por este motivo, cuando en el capítulo se habla de LVM nos referimos siempre a LVM2.

3.6.2. Configuración de LVM con YaST

La configuración de LVM mediante YaST se activa desde el módulo correspondiente de YaST (consulte la sección 2.7.5 en la página 73). Esta herramienta profesional de particionamiento le permite editar particiones ya existentes, borrarlas o

crear nuevas particiones. Desde aquí puede utilizar la opción 'Crear' → 'No formatear' y allí escoja el punto '0X8e Linux LVM'. Una vez que haya creado todas las particiones que serán utilizadas por LVM, pulse sobre 'LVM' para iniciar la configuración LVM.

Creación de grupos de volúmenes (VG)

Si aún no se ha creado ningún VG aparecerá una ventana que pide su creación (ver la figura **??** en esta página). 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 de un volumen físico dentro del grupo de volúmenes. Todo el espacio físico correspondiente a un grupo de volúmenes se gestiona a partir de este tamaño. 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 (por ejemplo a 8, 16 ó 32 megabytes), si no necesita volúmenes lógicos más grandes de 256 gigabytes.

Figura 3.2: *Creación de un grupo de volúmenes*

LVM: configuración de los volúmenes físicos

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. Una partición asignada a un VG se denomina volumen físico (Physical Volume o PV).

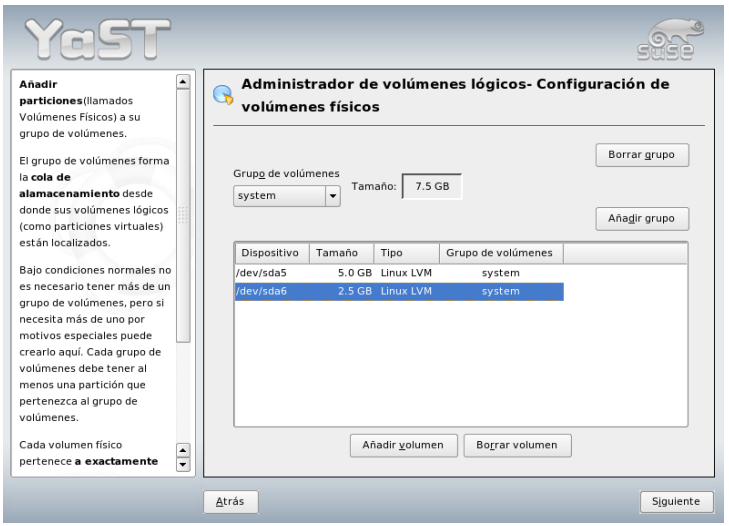

Figura 3.3: *Configuración de los volúmenes físicos*

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' 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. Una vez finalizado el proceso, pulse sobre 'Siguiente' para proceder a la configuración de los volúmemes lógicos.

Configuración de los volúmenes lógicos

Una vez que un grupo de volúmenes ha sido completado por volúmenes físicos, ha de definir qué volúmenes lógicos debe utilizar el sistema operativo. Seleccione el grupo de volúmenes deseado en la lista ubicada en la parte superior izquierda. Aquí también se muestra el espacio libre del grupo escogido. Esta lista contiene todos los volúmenes lógicos incluidos en el grupo. Asimismo, incluye 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. Añada, modifique o elimine los volúmenes lógicos según sus necesidades. Asigne al menos un volumen lógico a cada grupo de volúmenes.

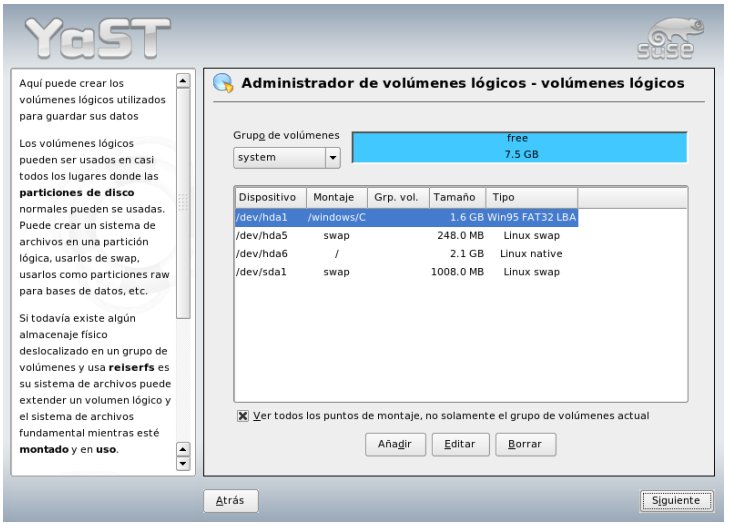

Figura 3.4: *Administración de volúmenes lógicos*

Para crear un nuevo volumen lógico, emplee el botón 'Añadir', indicando el tamaño, el tipo de sistema de archivos y el punto de anclaje. Sobre un volumen lógico se crea normalmente un sistema de archivos (por ejemplo reiserfs, ext2) y se asigna un punto de anclaje. Este es el punto de acceso para llegar posteriormente a los datos que se guardan sobre este volumen lógico. Asimismo, es posible distribuir el flujo de datos en los volúmenes lógicos entre varios volúmenes físicos (striping). Si los volúmenes físicos residen en varios discos duros, se observará generalmente un aumento en las prestaciones de lectura y escritura de datos (tal

como con RAID 0). Sin embargo, un LV con n bandas sólo puede crearse correctamente cuando el espacio de disco requerido por el LV puede distribuirse de forma uniforme en n volúmenes físicos. Si sólo están disponibles dos PVs, un LV con 3 bandas no sería viable.

Aviso

Striping

YaST no es capaz en este instante de verificar la exactitud de las entradas relacionadas con el striping. Cualquier error que se cometa en este punto sólo podrá advertirse cuando el LVM sea implementado en el disco.

Aviso

Figura 3.5: *Creación de volúmenes lógicos*

Si ya ha configurado LVM en el sistema, puede proceder seguidamente a introducir los volúmenes lógicos existentes. Antes de ello, asigne a cada uno de ellos un punto de montaje apropiado. Pulse sobre 'Siguiente' para regresar a YaST y finalizar el proceso de particionamiento.

Gestión directa LVM

Si ya ha configurado LVM y únicamente desea modificar algún aspecto, existe una alternativa para ello. Seleccione 'Sistema' → 'LVM' desde el centro de control de YaST. Este cuadro de diálogo le permite básicamente llevar a cabo las mismas acciones que las descritas anteriormente con la excepción del particionamiento físico. Esta opción muestra los volúmenes físicos y lógicos existentes agrupados en dos listas y le permite gestionar su sistema LVM empleando los métodos mencionados previamente.

3.7. La configuración de soft RAID

La idea de la tecnología RAID (Redundant Array of Inexpensive Disks) consiste en agrupar varias particiones para formar un disco duro *virtual* de grandes dimensiones y así optimizar el rendimiento, la seguridad de los datos o ambas cosas. La mayoría de las controladoras RAID suelen emplear el protocolo SCSI, ya que este es capaz de controlar un mayor número de discos duros de una forma más eficiente que el protocolo IDE. Además ofrece ventajas de cara al procesamiento de comandos en paralelo. Hoy en día ya existen algunas controladoras RAID que funcionan con discos duros IDE o SATA. Consulte a este respecto la base de datos de hardware en `http://cdb.suse.de`.

3.7.1. Soft RAID

Al igual que una controladora RAID, que puede resultar muy costosa, 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, una alternativa muy económica al hardware RAID. A la hora de combinar varios discos duros en un sistema RAID, RAID contempla diversas estrategias con objetivos, ventajas y características distintos. Estas estrategias se conocen comúnmente como niveles RAID o *RAID levels*.

Los niveles RAID más habituales son:

RAID 0 Este nivel mejora la velocidad de acceso a los datos mediante la diseminación de bloques de un archivo en varios discos. En realidad no se trata de un RAID porque no existe ninguna copia de seguridad de los datos pero la denominación *RAID 0* se ha hecho habitual para esta constelación de al menos dos discos duros. Si bien el rendimiento es alto, basta con que un disco falle para que el sistema RAID se estropee y todos los datos se pierdan.

RAID 1 Este nivel ofrece un nivel de seguridad aceptable para los datos porque se encuentran copiados con exactitud en otro disco duro. Este procedimiento se conoce como *hard disk mirroring* o 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 que se produzca una pérdida de datos. A causa del proceso de copia, la velocidad de escritura disminuye entre un 10 % y un 20 % con respecto al acceso a un único disco, pero la velocidad de lectura es bastante más alta porque los datos se pueden leer simultáneamente en varios discos. Se dice que el nivel 1 duplica la velocidad de transferencia de lectura de los sistemas con un solo disco y proporciona casi la misma velocidad de transferencia de escritura.

RAID 2 y RAID 3 Aquí no se trata de implementaciones RAID típicas. El RAID de nivel 2 distribuye los datos a nivel de bits y no por bloques. En el caso del nivel 3, los datos se fraccionan a nivel de bytes con un disco de paridad dedicada y no es posible procesar múltiples peticiones simultáneas. Estos niveles no suelen emplearse.

RAID 4 El nivel 4 combina la distribución de datos a nivel de bloques del nivel 0 con un disco de paridad dedicada. Si un disco de datos falla, los datos de paridad se utilizan para crear un nuevo disco que lo sustituya. A pesar de que el disco de paridad puede ocasionar embotellamientos en el acceso de escritura, el nivel 4 se usa en ocasiones.

RAID 5 RAID 5 constituye un compromiso optimizado entre los niveles 0 y 1 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 viene dada por la información de paridad que se encuentra en uno de los discos en el caso de RAID 5. Estos *bloques de paridad* se enlazan mediante un XOR lógico para conseguir la reconstrucción del contenido después de un fallo del sistema. En el caso de RAID 5 es vital que no falle nunca más de un disco duro al mismo tiempo. Un disco duro dañado debe ser reemplazado lo más rápidamente posible para evitar posibles pérdidas de datos.

Otros niveles RAID Existen otros niveles RAID (RAIDn, RAID 10, RAID 0+1, RAID 30, RAID 50, etc.), siendo algunos de ellos implementaciones propietarias desarrolladas por fabricantes de hardware. El uso de estos niveles no está muy extendido y por eso no se explican aquí.

3.7.2. Configuración de soft RAID con YaST

Puede acceder a la configuración de soft RAID con YaST a través de la herramienta de particionamiento en modo experto de YaST (ver sección 2.7.5 en la página 73). Esta herramienta le permite editar y borrar particiones existentes y crear otras nuevas que vayan a utilizarse con soft RAID. Para crear particiones RAID, pulse primero 'Crear' → 'No formatear' y seleccione a continuación '0xFD Linux RAID' como tipo de partición. Para RAID 0 y RAID 1 se requieren al menos dos particiones—para RAID 1 exactamente dos, ni más ni menos. Si se utiliza RAID 5 se requieren al menos tres particiones. Se recomienda utilizar particiones del mismo tamaño. Las particiones RAID deberían estar almacenadas en discos duros diferentes para reducir el riesgo de pérdida de datos en caso de fallo (RAID 1 y 5) y para optimizar el rendimiento de RAID 0. Una vez creadas todas las particiones que se van a usar con RAID, pulse 'RAID' → 'Crear RAID' para iniciar la configuración del RAID.

A continuación se abre un diálogo en el que puede seleccionar entre los niveles RAID 0, 1 y 5 (consulte la sección **??** en esta página para obtener información adicional). Pulsando 'Siguiente' accederá a una lista en la que aparecen todas las particiones de tipo "Linux RAID" o "Linux native" (ver figura **??** en esta página). Las particiones de intercambio o DOS no se muestran. Si una partición ya ha sido asignada a un volumen RAID, el nombre del dispositivo RAID (ej. `/dev/md0`) se incluye también en la lista. Las particiones sin asignar se identifican con "--".

Para añadir una partición sin asignar al volumen RAID seleccionado, pulse sobre la partición y a continuación en 'Añadir'. Al hacerlo, el nombre del dispositivo RAID aparecerá junto a la partición seleccionada. Se recomienda asignar todas las particiones reservadas para RAID. En caso contrario, el espacio de la partición no será utilizado. Después de asignar todas las particiones pulse en 'Siguiente' para acceder al diálogo de configuración donde puede ajustar diversos parámetros de rendimiento (ver figura **??** en esta página).

Como si de una partición convencional se tratara, defina en este diálogo el sistema de archivos que debe utilizarse así como el método de codificación y el punto de montaje para el volumen RAID. La activación de 'Superbloque persistente' garantiza que las particiones RAID se reconozcan como tales durante el arranque. Al completar la configuración con 'Finalizar', podrá ver el indicador *RAID* junto a `/dev/md0` y otros dispositivos en la herramienta de particionamiento en modo experto.

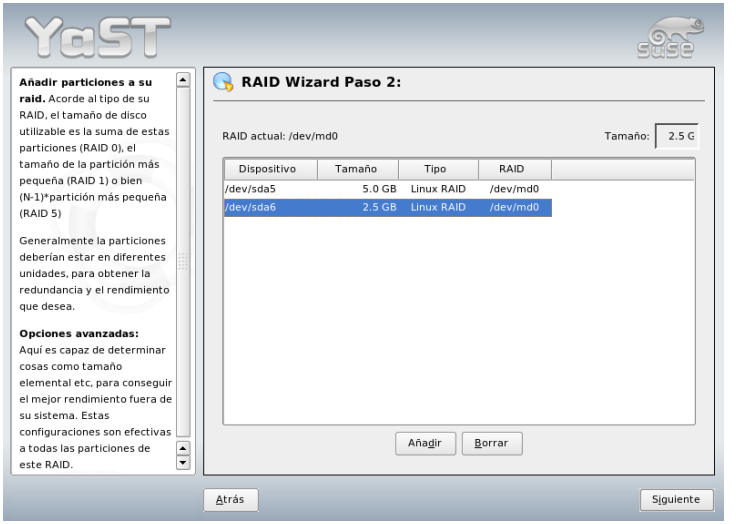

Figura 3.6: *Particiones RAID*

3.7.3. Resolución de problemas

El archivo `/proc/mdstats` informa sobre daños en una partición RAID. Si se ha producido un fallo del sistema, detenga el sistema Linux y sustituya el disco dañado por uno nuevo que contenga las mismas particiones. A continuación reinicie el sistema y ejecute el comando `mdadm /dev/mdX --add /dev/sdX`, reemplazando la 'X' por el identificador de dispositivo de su sistema. Este comando integra automáticamente el disco duro nuevo en el RAID y lo reconstruye.

3.7.4. Información adicional

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`

Figura 3.7: *Opciones de configuración del sistema de archivos*

o en la lista de correo de Linux RAID por ejemplo en `http://www.mail-archive.com/linux-raid@vger.rutgers.edu`.

Actualización del sistema y 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*. Los paquetes individuales también se pueden instalar manualmente con el gestor de paquetes RPM.

4.1. Actualización de SUSE LINUX

El software tiende a "crecer" 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 este depende en gran medida de las particiones actuales, del software elegido y de los números de versión de SUSE LINUX.

4.1.1. Preparativos

Antes de realizar cualquier actualización se deben copiar los archivos de configuración a un medio independiente (cinta, disco duro extraíble, unidad ZIP, etc.); sobre todo se trata de los archivos contenidos en `/etc` pero también se deben controlar y respaldar algunos de los directorios y archivos bajo `/var` o bajo `/opt`. Además se recomienda hacer una copia de seguridad de los datos actuales de los usuarios en `/home` (es decir, de 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 ejemplo **??** en esta página, `/dev/hda2` es la partición raíz que se debe anotar, ya que es ésta la que está montada como `/`.

Ejemplo 4.1: *Salida de* `df -h`

```
Filesystem  Size  Used Avail Use% Mounted on
/dev/hda1   1,9G  189M  1.7G  10%  /dos
/dev/hda2   8,9G  7,1G  1,4G  84%  /
/dev/hda5   9,5G  8,3G  829M  92%  /home
```

4.1.2. Posibles problemas

Comprobación de passwd y group en /etc

Antes de actualizar el sistema hay que asegurarse de que los archivos `/etc/passwd` y `/etc/group` estén libres de errores de sintaxis. Para comprobarlo, ejecute como `root` los programas `pwck` y `grpck` y corrija los errores que aparezcan.

PostgreSQL

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

4.1.3. Actualización con YaST

Una vez realizados los preparativos descritos en la sección **??** en esta página, puede iniciar el proceso de arranque:

1. Inicie el sistema como para la instalación según se describe en la sección 1.1 en la página 4. 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 se continúa con la copia de seguridad del sistema. En caso de que existan varias particiones, seleccione la partición correcta y confirme con 'Siguiente'. En el ejemplo de la sección ?? en esta página seleccionó `/dev/hda2`. YaST lee también 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.

4.1.4. Actualización de paquetes individuales

Independientemente de la actualización del sistema base, se pueden actualizar paquetes sueltos en cualquier momento. Realizando una actualización parcial, *usted mismo* debe encargarse de mantener la consistencia del sistema en cuanto a las dependencias de los paquetes. Puede encontrar algunos consejos sobre la actualización en `http://www.novell.com/linux/download/updates/`.

En la selección de paquetes de YaST puede seleccionar y deseleccionar paquetes como le plazca. Al seleccionar un paquete esencial para el sistema, YaST advierte sobre la necesidad de actualizar dicho paquete en el modo especial de actualización. Por ejemplo, hay muchos paquetes que utilizan bibliotecas compartidas (shared libraries) que pueden estar en uso en el momento de la actualización. Por tanto, algunos programas podrían dejar de funcionar correctamente después de realizar una actualización desde el sistema activo.

4.2. Cambios en el software de una versión a otra

En los siguientes apartados se describen los aspectos que han cambiado de una versión a otra de SUSE LINUX, como por ejemplo el cambio de ubicación de un archivo de configuración o una modificación importante de un programa conocido. En estas líneas se mencionan los aspectos que atañen directamente a los usuarios o administrador de sistemas en su trabajo diario.

Los problemas y cambios de última hora de cada versión se publican en nuestro servidor web; véase a este fin los enlaces en las líneas inferiores. Se puede actualizar determinados paquetes importantes a través de `http://www.novell.com/products/linuxprofessional/downloads/` o por medio de la actualización en línea de YaST (YOU)—ver sección 2.2.3 en la página 49.

4.2.1. De 8.2 a 9.0

Problemas y peculiaridades: `http://portal.suse.com/sdb/en/2003/07/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 **??** en esta página.
- El paquete `footmatic-filters` está disponible para la impresión. Su 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/lpdfilter se requieren los paquetes `footmatic-filters` y `cups-drivers`.
- Es posible acceder 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 de ser así los comentarios organizativos desaparecerán. 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.

4.2.2. De 9.0 a 9.1

Consulte el artículo "Known Problems and Special Features in SUSE LINUX 9.1" disponible en la base de datos de soporte de SUSE en `http://portal.suse.de`. Para acceder al artículo puede emplear la palabra clave *bugs*. Para todas las versiones de SUSE LINUX se redacta un artículo de este tipo.

Actualización al kernel 2.6

SUSE LINUX se basa completamente en la versión 2.6 del kernel. La versión anterior, 2.4, no debería seguir utilizándose ya que los programas incluidos podrían no funcionar con el kernel 2.4. Asimismo es necesario tener en cuenta lo siguiente:

- La carga de los módulos se configura en el archivo `/etc/modprobe.conf`, el archivo `/etc/modules.conf` ha quedado obsoleto. YaST intenta convertir dicho archivo (véase también el script `/sbin/generate-modprobe.conf`).
- Los módulos tienen la extensión `.ko`.
- El módulo `ide-scsi` ya no es necesario para grabar CDs.
- El prefijo `snd_` se ha eliminado de las opciones del módulo de sonido ALSA.
- `sysfs` complementa al sistema de archivos `/proc`.
- La gestión de energía (y en particular ACPI) ha sido perfeccionada y puede configurarse mediante un módulo de YaST.

Montaje de particiones VFAT

Hay que cambiar el parámetro `code=` a `codepage=` para montar particiones VFAT. Si hay problemas montando una partición VFAT, compruebe que no se utilice el parámetro antiguo en el archivo `/etc/fstab`.

Standby/Suspend con ACPI

El kernel 2.6 soporta ahora los modos standby y suspend con ACPI. Es una función aún experimental y no funciona con todo el hardware. Para utilizarlo hace falta instalar el paquete `powersave`. Puede obtener información adicional sobre este paquete en `/usr/share/doc/packages/powersave`. El paquete `kpowersave` contiene una interfaz gráfica.

Dispositivos de entrada (input devices)

Respecto al cambio de dispositivos de entrada, consulte el artículo "Known Problems and Special Features in SUSE LINUX 9.1" mencionado anteriormente al que puede acceder en la base de datos de soporte `http://portal.suse.de` con la palabra clave *bugs*.

Native POSIX Thread Library y glibc 2.3.x

Los programas que están enlazados con NGPT (*Next Generation POSIX Threading*) no funcionan con glibc 2.3.x. Todos los programas afectados que no estén incluidos en SUSE LINUX deben volver a compilarse con linuxthreads o bien con NPTL (*Native POSIX Thread Library*). Se recomienda portarlos con NPTL, ya que éste se anticipa como el estándar del futuro.

En caso de problemas con NPTL, puede utilizar la implementación linuxthreads, algo más antigua, mediante la asignación de las siguientes variables de entorno (debe sustituir ⟨*kernel-version*⟩ por el número de versión del kernel en cuestión):

```
LD_ASSUME_KERNEL=kernel-version
```

Los números de versión posibles son los siguientes:

2.2.5 (i386, i586): linuxthreads sin floating stacks

2.4.1 (AMD64, i586, i686): linuxthread con floating stacks

Observaciones respecto al kernel y linuxthreads *con* floating stacks: los programas que utilizan `errno`, `h_errno` y `_res`, deben integrar los archivos correspondientes de la cabecera (`errno.h`, `netdb.h` y `resolv.h`) por medio de `#include`. En el caso de los programas C++- con soporte multithread que usen *thread cancellation*, debe utilizarse la variable de entorno `LD_ASSUME_KERNEL=2.4.1` para forzar el uso de la biblioteca linuxthreads.

Modificaciones para Native POSIX Thread Library

NPTL se incluye en SUSE LINUX 9.1 como paquete de hilos. NPTL ha sido desarrollado de forma que los binarios son compatibles con los de la antigua biblioteca linuxthreads. No obstante, donde linuxthreads contraviene el estándar POSIX, NPTL requiere algunas modificaciones. En particular cabe mencionar las siguientes: manejo de señales, `getpid` devuelve un valor idéntico en todos los hilos, los gestores de hilos (thread handler) registrados con pthread_atfork no se ejecutan al utilizar `vfork`.

Configuración de la interfaz de red

La configuración de la interfaz de red se ha modificado. Hasta ahora, el hardware se iniciaba después de configurar una interfaz aún no existente. Ahora, el sistema busca hardware nuevo y lo inicia inmediatamente, permitiendo la configuración de la nueva interfaz de red.

Los nombres de los archivos de configuración han cambiado. Considerando la amplia difusión de dispositivos hotplug, los nombres como `eth0` o `eth1` ya no son adecuados a efectos de configuración porque se crean de forma dinámica. Por eso ahora se utilizan identificadores únicos como la dirección MAC o la ranura PCI para denominar a la interfaz. No obstante, aún es posible utilizar comandos como `ifup eth0` o `ifdown eth0`.

Las configuraciones de dispositivos se encuentran en `/etc/sysconfig/hardware`. Las interfaces proporcionadas por los dispositivos suelen estar (con nombres diferentes) en `/etc/sysconfig/network`. Véase también la descripción detallada en `/usr/share/doc/packages/sysconfig/README`.

Configuración de sonido

Las tarjetas de sonido se tienen que configurar nuevamente después de una actualización. Esto se realiza con el módulo de sonido de YaST. Introduzca como `root` el comando `yast2 sound`.

Dominio de primer nivel .local como dominio de enlace local

La biblioteca de resolución trata el dominio de primer nivel (top-level domain) `.local` como dominio de enlace local ("link-local" domain) y envía consultas de DNS del tipo multicast a la dirección multicast `224.0.0.251` puerto `5353` en lugar de realizar consultas DNS normales. Esto es una modificación incompatible. Por eso tiene que utilizar otro dominio si ya está utilizando `.local` en la configuración del servidor de nombres. Más información sobre DNS multicast en `http://www.multicastdns.org`.

UTF-8 como codificación global del sistema

`UTF-8` es la codificación predeterminada para el sistema. Así, en la instalación estándar se define una configuración local con `UTF-8` como indicación de codificación (*encoding*), por ejemplo, `es_ES.UTF-8`. Más información en: `http://www.suse.de/~mfabian/suse-cjk/locales.html`.

Conversión de nombres de archivos a UTF-8

Los archivos de sistemas de archivos creados anteriormente no suelen utilizar la codificación UTF-8 en sus nombres. Si estos contienen caracteres no ASCII, se mostrarán con errores. Para corregir este problema utilice el script `convmv`, que convierte la codificación de los nombres a UTF-8.

Herramientas de shell compatibles con el estándar POSIX de 2001

Algunas de las herramientas de la shell incluidas en el paquete `coreutils` tales como `tail`, `chown`, `head`, `sort`, etc. han abandonado el el estándar de 1992 y siguen ahora el estándar POSIX de 2001 (*Single UNIX Specification, version 3 == IEEE Std 1003.1-2001 == ISO/IEC 9945:2002*). El antiguo comportamiento puede reproducirse con una variable de entorno:

```
_POSIX2_VERSION=199209
```

El nuevo valor es 200112 y se adopta como valor predeterminado para `_POSIX2_VERSION`. El estándar SUS puede consultarse (gratuitamente pero de registro obligatorio) en `http://www.unix.org`

Cuadro 4.1: *Comparación entre POSIX 1992 y POSIX 2001*

POSIX 1992	POSIX 2001
chown tux.users	chown tux:users
tail +3	tail -n 3
head -1	head -n 1
sort +3	sort -k 4
nice -10	nice -n 10
split -10	split -l 10

Sugerencia

Es posible que el software de terceros fabricantes todavía no siga el nuevo estándar. En estos casos se recomienda definir la variable de entorno como se describe en líneas superiores.

Sugerencia

/etc/gshadow obsoleto

`/etc/gshadow` ha sido eliminado ya que ha quedado obsoleto. Los motivos para tomar esta decisión han sido los siguientes:

- glibc no lo soporta.
- No existe ninguna interfaz oficial para este archivo, ni siquiera en la suite shadow.
- La mayor parte de las herramientas que comprueban las contraseñas de grupo no soportan este archivo y lo ignoran por las razones ya mencionadas.

OpenLDAP

Debido a que el formato de las bases de datos ha cambiado, éstas han de volver a generarse. Durante la actualización se lleva a cabo una conversión automática, pero es casi seguro que existan casos en los que esta conversión fracase.

La comprobación de esquemas ha experimentado importantes mejoras. Por este motivo puede haber ciertas operaciones no conformes con el estándar que, si bien eran admitidas anteriormente por el servidor LDAP, han dejado de serlo.

La sintaxis del archivo de configuración se modificó parcialmente con miras a las ACL. Después de la instalación, puede obtener información adicional sobre la actualización de LDAP en el archivo: `/usr/share/doc/packages/openldap2/README.update`

Apache 2 sustituye a Apache 1.3

El servidor web Apache (versión 1.3) ha sido sustituido por Apache 2. Encontrará abundante documentación sobre la versión 2.0 de este programa en la página web `http://httpd.apache.org/docs-2.0/es/`. Al actualizar un sistema en el que esté instalado un servidor HTTP, se borrará el paquete Apache y se instalará Apache 2. Posteriormente habrá que ajustar manualmente el sistema con YaST. Los archivos de configuración almacenados en `/etc/httpd` se encuentran ahora en `/etc/apache2`.

En Apache 2 existe la posibilidad de utilizar threads (hilos) o procesos para ejecutar simultáneamente varias solicitudes. La administración de procesos se produce en un módulo propio, el módulo multiproceso o MPM. Asimismo, Apache 2 requiere el paquete `apache2-prefork` (recomendado a efectos de estabilidad) o bien `apache2-worker`. Apache 2 reacciona de forma distinta a las solicitudes dependiendo del MPM. Las diferencias se reflejan en el rendimiento y en la utilización de los módulos. Estas características se explican con más detalle en la sección **??** en esta página.

Apache 2 soporta el protocolo de Internet de última generación 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 suele ser muy importante y antiguamente se determinaba en función del orden de carga. Así, un módulo que sólo permita acceder a determinados recursos a los usuarios autentificados debe activarse en primer lugar para que los usuarios sin permiso de acceso no lleguen a ver las páginas.

Las solicitudes a Apache y sus respuestas pueden procesarse con filtros.

De Samba 2.x a Samba 3.x

Con la actualización de Samba 2.x a Samba 3.x se ha suprimido la autenticación por `winbind`. Los demás métodos de autenticación siguen existiendo, por lo que se han eliminado los siguientes programas:

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

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

Actualización de OpenSSH (Version 3.8p1)

El soporte `gssapi` ha sido reemplazado por `gssapi-with-mic` para evitar posibles ataques del tipo MITM. Las dos versiones no son compatibles y por eso no es posible la autenticación desde distribuciones anteriores con tickets de kerberos. Los métodos de autenticación han cambiado.

Aplicaciones de terminal y SSH

Las aplicaciones de terminal pueden mostrar caracteres erróneos cuando se está realizando un acceso desde un ordenador remoto vía SSH, telnet o RSH y uno de los ordenadores utiliza la versión 9 (en su configuración estándar con UTF-8 activado) mientras que el otro tiene un sistema antiguo (SUSE LINUX 9.0 ó anterior sin activación o soporte de UTF-8).

OpenSSH no transmite la configuración local, por lo que se utiliza la configuración predeterminada del sistema. Estas pueden diferir de las de la terminal remota. Es el caso de YaST en modo texto y aplicaciones que se ejecutan desde un ordenador remoto como usuario normal (no como `root`) Las aplicaciones ejecutadas por `root` sólo tienen este problema cuando la configuración estándar local se ha modificado para `root` (sólo `LC_CTYPE` se configura por defecto).

libiodbc ha sido suprimida

Los usuarios de FreeRADIUS tienen que enlazar ahora con unixODBC en lugar de libiodbc, ya que esta última biblioteca ha sido suprimida.

Recursos XML en /usr/share/xml

El estándar FHS (ver sección **??** en esta página) prevé que los recursos XML (DTDs, hojas de estilo, etc.) se instalen en `/usr/share/xml`. Por este motivo, algunos directorios ya no se encuentran en `/usr/share/sgml`. En caso de problemas debe modificar sus propios scripts y makefiles, o bien utilizar los catálogos oficiales (en particular `/etc/xml/catalog` o `/etc/sgml/catalog`).

Medios de almacenamiento extraíbles con subfs

Los medios de almacenamiento extraíbles se integran ahora vía subfs. Ya no hace falta montar el medio manualmente (`mount`), sino que basta con cambiar al directorio correspondiente en `/media` para montar el medio. No se puede desmontar o expulsar un medio mientras un programa esté accediendo a él.

4.2.3. De 9.1 a 9.2

Consulte el artículo "Known Problems and Special Features in SUSE LINUX 9.2" de la base de datos de soporte de SUSE en `http://portal.suse.de`. Para acceder a este artículo, utilice la palabra clave *bugs*.

Activación del cortafuegos en el diálogo de propuestas durante la instalación

SuSEFirewall2, la solución cortafuegos incluida en la distribución, se activa en el diálogo de propuestas al final de la instalación para incrementar el nivel de seguridad. Esto significa que en un principio todos los puertos están cerrados y pueden abrirse a petición del usuario al comienzo del diálogo de propuestas. Por ejemplo, no es posible registrarse en el sistema desde un equipo remoto usando la configuración predeterminada. Asimismo, esto puede interferir en la navegación en redes y en el uso de aplicaciones de multidifusión o multicast como SLP, Samba ("Network Neighborhood") y algunos juegos. YaST le permite configurar el cortafuegos de forma detallada.

Si durante la instalación o configuración de un servicio se requiere una conexión a la red, el módulo de YaST correspondiente abre los puertos TCP y UDP necesarios en todas las interfaces internas y externas. Si el usuario no está de acuerdo con esta acción, puede cerrar los puertos en el módulo de YaST o bien modificar la configuración del cortafuegos.

Cuadro 4.2: *Puertos requeridos por los principales servicios*

Servicio	Puertos
Servidor HTTP	cortafuegos configurado conforme a las declaraciones "listen" (sólo TCP)
Correo (postfix)	smtp 25/TCP
Servidor Samba	netbios-ns 137/TCP; netbios-dgm 138/TCP; netbios-ssn 139/TCP; microsoft-ds 445/TCP

Servidor DHCP	bootpc 68/TCP
Servidor DNS	domain 53/TCP; domain 53/UDP
Servidor DNS	más soporte especial para el mapeador de puertos en SuSEFirewall2
Mapeador de puertos	sunrpc 111/TCP; sunrpc 111/UDP
Servidor NFS	nfs 2049/TCP
Servidor NFS	más mapeador de puertos
Servidor NIS	activa portmap
TFTP	tftp 69/TCP
CUPS (IPP)	ipp 631/TCP; ipp 631/UDP

KDE y el soporte IPv6

El soporte IPv6 no está activado de forma estándar en KDE. Puede activarlo con el editor `/etc/sysconfig` de YaST. El motivo de esta desactivación es que no todos los proveedores de servicios de Internet soportan correctamente las direcciones IPv6. En consecuencia, la activación predeterminada podría ocasionar mensajes de error al navegar por Internet y retrasos al cargar páginas web.

YaST Online Update y los "paquetes delta"

YaST Online Update soporta un tipo especial de paquetes RPM en los que sólo se guarda la diferencia binaria con un paquete base determinado. Gracias a esta técnica se reduce sustancialmente el tamaño del paquete y por consiguiente el tiempo de descarga, a expensas de una mayor carga de la CPU a la hora de montar el paquete final. En `/etc/sysconfig/onlineupdate` puede configurar si YOU debe emplear estos "paquetes delta". Para obtener información adicional de carácter técnico, consulte el archivo `file:///usr/share/doc/packages/deltarpm/README`.

Configuración del sistema de impresión

Al final de la instalación (diálogo de propuestas), debe asegurarse de que los puertos requeridos por el sistema de impresión están abiertos en la configuración del cortafuegos. Los puertos 631/TCP y 631/UDP son necesarios para CUPS

y no pueden estar cerrados durante una operación normal. De igual forma, debe ser posible acceder al puerto 515/TCP (para el antiguo protocolo LPD) o a los puertos requeridos por Samba para imprimir mediante LPD o SMB.

Migración a X.Org

La migración de XFree86 a X.Org se ha simplificado a través de enlaces de compatibilidad. Gracias a estos enlaces, aún es posible acceder a los principales archivos y comandos por medio de los nombres antiguos.

Cuadro 4.3: *Comandos*

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

Cuadro 4.4: *Archivos de registro en /var/log*

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

Además, los paquetes de `XFree86*` han pasado a llamarse `xorg-x11*` en el marco de la migración a X.Org.

Emuladores de terminal para X11

Hemos eliminado de la distribución algunos emuladores de terminal que o bien han dejado de mantenerse o no funcionan en el entorno estándar, especialmente por no soportar UTF-8. SUSE LINUX incorpora terminales estándar como por ejemplo xterm, los terminales de KDE y GNOME y mlterm (Multilingual Terminal Emulator for X), que puede emplearse en lugar de aterm y eterm.

Cambios en el paquete powersave

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

Cuadro 4.5: *Distribución en los archivos de configuración de /etc/sysconfig/powersave*

Archivo anterior	Ahora dividido en
`/etc/sysconfig/powersave/common`	`common`
	`cpufreq`
	`events`
	`battery`
	`sleep`
	`thermal`

El archivo `/etc/powersave.conf` ya no existe y las variables han sido trasladadas a los archivos mencionados en la tabla **??** en esta página. En caso de haber efectuado cambios en las variables "event" del archivo `/etc/powersave.conf`, estos han de realizarse ahora en `/etc/sysconfig/powersave/events`.

Asimismo se ha modificado la nomenclatura de los "estados de sueño" (sleep status). Nomenclatura anterior:

- suspend (ACPI S4, APM suspend)
- standby (ACPI S3, APM standby)

Nomenclatura actual:

- suspend to disk (ACPI S4, APM suspend)
- suspend to ram (ACPI S3, APM suspend)
- standby (ACPI S1, APM standby)

OpenOffice.org (OOo)

Directorios: OOo se instala ahora en `/usr/lib/ooo-1.1` en lugar de en `/opt/OpenOffice.org`. El directorio donde se guarda la configuración de usuario ya no es `~/OpenOffice.org1.1` sino `~/.ooo-1.1`.

Wrapper: Existen nuevos wrappers para iniciar los componentes de OOo. Los nuevos nombres se muestran en la tabla **??** en esta página.

Cuadro 4.6: *Wrapper*

Antiguo	Nuevo
`/usr/X11R6/bin/OOo-calc`	`/usr/bin/oocalc`
`/usr/X11R6/bin/OOo-draw`	`/usr/bin/oodraw`
`/usr/X11R6/bin/OOo-impress`	`/usr/bin/ooimpress`
`/usr/X11R6/bin/OOo-math`	`/usr/bin/oomath`
`/usr/X11R6/bin/OOo-padmin`	`/usr/sbin/oopadmin`
`/usr/X11R6/bin/OOo-setup`	–
`/usr/X11R6/bin/OOo-template`	`/usr/bin/oofromtemplate`
`/usr/X11R6/bin/OOo-web`	`/usr/bin/ooweb`
`/usr/X11R6/bin/OOo-writer`	`/usr/bin/oowriter`
`/usr/X11R6/bin/OOo`	`/usr/bin/ooffice`
`/usr/X11R6/bin/OOo-wrapper`	`/usr/bin/ooo-wrapper`

Como novedad, el wrapper soporta ahora la opción `--icons-set` para cambiar entre los iconos de KDE y GNOME. Las opciones que han dejado de soportarse son `--default-configuration`, `--gui`, `--java-path`, `--skip-check`, `--lang` (ahora se utiliza locales) para determinar el idioma), `--messages-in-window` y `--quiet`.

Soporte para KDE y GNOME: OpenOffice.org incorpora ahora soporte ampliado para KDE y GNOME que se incluye en los paquetes `OpenOffice_org-kde` y `OpenOffice_org-gnome`.

Mezclador de sonido "kmix"

El mezclador de sonido kmix es la opción predeterminada. También dispone de mezcladores alternativos como QAMix/KAMix, envy24control (sólo ICE1712) o hdspmixer (sólo RME Hammerfall) para el hardware de gama alta.

Grabación de DVDs

En versiones anteriores aplicamos un parche al binario `cdrecord` del paquete `cdrecord` para soportar la grabación de DVDs. En su lugar, en esta versión se instala un nuevo binario, `cdrecord-dvd`, que ya contiene este parche.

El programa `growisofs` del paquete `dvd+rw-tools` ya puede grabar todos los medios de DVD (DVD+R, DVD-R, DVD+RW, DVD-RW, DVD+RL). Le recomendamos utilizar dicho programa en vez del binario parcheado `cdrecord-dvd`.

Varios kernels

Es posible instalar múltiples kernels de forma paralela. El propósito de esta prestación consiste en permitir a los administradores actualizar de un kernel a otro instalando primero un nuevo kernel, comprobando si dicho kernel funciona y desinstalando el kernel antiguo. Si bien YaST todavía no soporta esta función, los kernels pueden instalarse y desinstalarse fácilmente desde la shell por medio del comando `rpm -i` ⟨*paquete*⟩`.rpm`. Puede obtener información adicional sobre la gestión de paquetes desde la línea de comandos en la sección **??** en esta página.

Los menús predeterminados del cargador de arranque contienen una entrada para el kernel. Antes de instalar varios kernels se recomienda añadir una entrada para los kernels adicionales de forma que puedan seleccionarse fácilmente. Puede acceder al kernel que estaba activo anteriormente por medio de `vmlinuz.previous` e `initrd.previous`, es decir, creando una entrada de cargador de arranque similar a la entrada predeterminada pero denominada `vmlinuz.previous` o `initrd.previous` en lugar de `vmlinuz` o `initrd`. Asimismo, GRUB y LILO soportan entradas comodín en el cargador de arranque. Para obtener más información al respecto, consulte las páginas info de GRUB (`info grub`) y la página man (5) de `lilo.conf`.

4.2.4. De 9.2 a 9.3

Consulte el artículo "Known Problems and Special Features in SUSE LINUX 9.3" de la base de datos de soporte de SUSE en `http://portal.suse.com`. Para acceder a este artículo, utilice la palabra clave *bugs*.

Inicio de la instalación manual en el prompt del kernel

El modo 'Manual Installation' ha desaparecido de la pantalla del cargador de arranque. Para iniciar linuxrc en modo manual, introduzca la opción `manual=1` en el prompt de arranque. Normalmente no es necesario, ya que es posible definir directamente en el prompt del kernel opciones de instalación como `textmode=1` o una URL como fuente de instalación.

Kerberos para la autenticación de red

`Kerberos` ha sustituido a `heimdal` como mecanismo estándar para la autenticación de redes. No es posible convertir automáticamente una configuración existente de heimdal. Al actualizar el sistema se crearán copias de seguridad de los archivos de configuración como se muestra en la tabla **??** en esta página.

Cuadro 4.7: *Copias de seguridad de archivos*

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

La configuración del cliente (`/etc/krb5.conf`) es muy parecida a la de heimdal. Si no se ha definido ninguna configuración especial, basta con sustituir el parámetro `kpasswd_server` por `admin_server`.

No es posible adoptar los datos relacionados con el servidor (kdc/kadmind) en el nuevo sistema. Tras la actualización del sistema, la antigua base de datos de heimdal sigue estando disponible en `/var/heimdal`. Por su parte, MIT kerberos mantiene su base de datos en `/var/lib/kerberos/krb5kdc`.

Archivo de configuración de X.Org

La herramienta de configuración SaX2 escribe la configuración de X.Org en el archivo `/etc/X11/xorg.conf`. Si se realiza una instalación desde cero, no se crea ningún enlace de compatibilidad entre `XF86Config` y `xorg.conf`.

Configuración de PAM

`common-auth` Configuración predeterminada de PAM para la sección auth.

common-account Configuración predeterminada de PAM para la sección account.

common-password Configuración predeterminada de PAM para el cambio de constraseñas.

common-session Configuración predeterminada de PAM para la administración de sesiones.

Se recomienda incluir estos archivos de configuración predeterminada en el archivo de configuración de las aplicaciones específicas, ya que resulta más sencillo modificar y mantener un único archivo de configuración que los 40 archivos que solía haber en el sistema. Las aplicaciones instaladas posteriormente heredarán los cambios ya aplicados sin que el administrador tenga que ajustar la configuración manualmente cada vez.

Los cambios son muy sencillos. Supongamos que dispone del siguiente archivo de configuración (que será el archivo predeterminado para la mayoría de aplicaciones):

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

Para incluir los archivos de configuración predeterminados, cámbielo a:

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

4.3. El gestor de paquetes RPM

SUSE LINUX utiliza RPM (Red Hat Package Manager) con sus principales programas `rpm` y `rpmbuild` para la administración de los paquetes de software.

Esta potente base de datos puede ser consultada tanto por usuarios como por administradores de sistemas o constructores de paquetes para obtener información detallada 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 (pristine sources).

Los archivos RPM instalables 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. Puede obtener información adicional sobre LSB en la sección ?? en esta página.

Sugerencia

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; por ejemplo compilar paquetes de GNOME más recientes. Este tipo de paquetes se identifica normalmente con el sufijo `-devel` en su nombre; algunos ejemplos son: `alsa-devel`, `gimp-devel`, `kdelibs-devel`, etc.

Sugerencia

4.3.1. Comprobar la autenticidad de un paquete

Los paquetes RPM de SUSE LINUX están firmados con GnuPG. La clave incluyendo huella digital (fingerprint) es la siguiente:

```
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` permite comprobar la firma de un paquete RPM para averiguar si éste procede realmente de SUSE u

otra entidad de. Este procedimiento se recomienda especialmente con los paquetes de actualización de Internet. Nuestra clave pública para firmar los paquetes se encuentra normalmente en `/root/.gnupg/`. 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.

4.3.2. Administración de paquetes: instalar, actualizar y desinstalar paquetes.

Por lo general, la instalación de un archivo RPM es muy simple: `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 poner en peligro la posibilidad de actualizar el paquete.

Las opciones `-U` o `--upgrade` y `-F` o `--freshen` pueden utilizarse para la actualización de un paquete, por ejemplo: `rpm -F` ⟨*`paquete`*⟩`.rpm`. Este comando borra la antigua versión de un paquete e instala los archivos nuevos. La diferencia entre ambas opciones radica en que en el caso de `-U` también se instalan paquetes que hasta ahora no estaban disponibles en en el sistema, mientras que la opción `-F` sólo actualiza un paquete que ya estuviera instalado. Por su parte, `rpm` actualiza los *archivos de configuración* cuidadosamente 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`.
- Los 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 `.rpmsave` y `.rpmnew` para que estos no obstaculicen la siguiente actualización. La extensión `.rpmorig` se aplica cuando la base de datos RPM no ha reconocido el archivo.

Si la base de datos reconoce el archivo se utiliza `.rpmsave`. En otras palabras, la extensión `.rpmorig` se genera cuando se actualizan paquetes de otro formato a RPM y `.rpmsave` se genera cuando se actualiza de un paquete RPM antiguo a uno más actual. La extensión `.rpmnew` se usa cuando no se puede determinar si el administrador de sistema ha modificado el archivo de configuración o no. Puede encontrar una lista de estos archivos en `/var/adm/rpmconfigcheck`. Algunos archivos de configuración (como `/etc/httpd/httpd.conf`) no se sobreescriben para posibilitar la operación continua.

Así pues, la opción `-U` (update) es algo más que una equivalencia de la secuencia `-e` (desinstalar/eliminar) e `-i` (instalar). Siempre que sea posible, es preferible usar la opción `-U`.

Para eliminar un paquete ejecute `rpm -e` ⟨*`paquete`*⟩. `rpm` sólo borra un paquete en caso de no existir ninguna dependencia. Por lo tanto no es posible suprimir por ejemplo 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`.

4.3.3. 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 en archivos pequeños, podíamos encontrarnos rápidamente ante una gran cantidad de datos. No obstante, el RPM de SUSE incorpora una función que permite instalar parches en paquetes.

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

¿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 se realiza con el comando

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

A continuación examine 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 sobre qué versiones de paquetes se han instalado?

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 las prestaciones de los parches) en las páginas del manual de `rpm` y `rpmbuild`.

4.3.4. Los paquetes RPM delta

Los paquetes "RPM delta" contienen la diferencia (denominada "delta") entre las versiones nueva y antigua de un paquete RPM. Si se aplica un RPM delta a un RPM antiguo, el resultado es un RPM completamente nuevo. No obstante, no es necesario tener una copia del antiguo RPM: un RPM delta también funciona con el RPM instalado. Los paquetes deltarpm son incluso más pequeños que los parches RPM, lo cual constituye una ventaja a la hora de transferir paquetes de actualización por Internet. Su principal inconveniente radica en que las actualizaciones con RPMs delta consumen bastante más ciclos de CPU que las actualizaciones con RPMs normales o parches. Si desea que YaST utilice paquetes RPM delta en las actualizaciones con YOU, asigne el valor "yes" a la opción `YOU_USE_DELTAS` en el archivo `/etc/sysconfig/onlineupdate`.

Los binarios `prepdeltarpm`, `writedeltarpm` y `applydeltarpm` forman parte de la suite deltarpm y su labor es la de facilitar la creación y aplicación de los paquetes RPM delta. Con los comandos siguientes puede crear un RPM delta llamado `new.delta.rpm` (este comando asume que tanto `old.rpm` como `new.rpm` están presentes):

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

xdelta delta -0 old.cpio new.cpio delta

writedeltarpm new.rpm delta info new.delta.rpm
rm old.cpio new.cpio delta
```

El comando `applydeltarpm` le permite reconstruir el nuevo RPM, ya sea desde el sistema de archivos en caso de que el paquete antiguo esté instalado:

```
applydeltarpm new.delta.rpm new.rpm
```

o bien con la opción `-r` para reconstruirlo a partir del antiguo RPM pero sin acceder al sistema de archivos:

```
applydeltarpm -r old.rpm new.delta.rpm new.rpm
```

Consulte `file:///usr/share/doc/packages/deltarpm/README` para obtener información adicional de carácter técnico.

4.3.5. Consultas RPM

La opción `-q` (query) permite enviar consultas a los archivos RPM (opción `-p` ⟨*archivo_paquete*⟩), así como a la base de datos RPM. Existen varias opciones para especificar el tipo de información requerida (tabla **??** en esta página).

Cuadro 4.8: *Las principales opciones para consultas RPM*

`-i`	Mostrar información sobre un paquete
`-l`	Mostrar lista de archivos del paquete
`-f Archivo`	Consultar el paquete que contiene el archivo ⟨*Archivo*⟩; se requiere la especificación de ⟨*Archivo*⟩ con su rama completa.
`-s`	Mostrar estado de los archivos (implica `-l`)
`-d`	Nombrar archivos de documentación (implica `-l`)
`-c`	Nombrar archivos de configuración (implica `-l`)
`--dump`	Mostrar toda la información de verificación de todos los archivos (utilizarlo con `-l`, `-c` o `-d`)
`--provides`	Mostrar prestaciones del paquete que otro paquete puede solicitar con `--requires`
`--requires`, `-R`	Mostrar dependencias entre los paquetes
`--scripts`	Mostrar los distintos scripts de instalación (preinstall, postinstall, uninstall)

Por ejemplo, el comando `rpm -q -i wget` produce como resultado la información postrada en el ejemplo **??** en esta página.

Ejemplo 4.2: *rpm -q -i wget*

```
Name        : wget                      Relocations: (not relocatable)
Version     : 1.9.1                          Vendor: SUSE LINUX AG, Nuernberg, Germany
Release     : 50                         Build Date: Sat 02 Oct 2004 03:49:13 AM CEST
Install date: Mon 11 Oct 2004 10:24:56 AM CEST      Build Host: f53.suse.de
Group       : Productivity/Networking/Web/Utilities Source RPM: wget-1.9.1-50.src.rpm
Size        : 1637514                      License: GPL
Signature   : DSA/SHA1, Sat 02 Oct 2004 03:59:56 AM CEST, Key ID a84edae89c800aca
Packager    : http://www.suse.de/feedback
URL         : http://wget.sunsite.dk/
Summary     : A tool for mirroring FTP and HTTP servers

Description :
Wget enables you to retrieve WWW documents or FTP files from a server.
This might be done in script files or via command line.
[...]
```

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
```

produce como resultado:

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

Si sólo se conoce una parte del nombre del archivo, utilice un script de shell como el mostrado en el ejemplo **??** en esta página) pasándole como parámetro el nombre del archivo buscado.

Ejemplo 4.3: *Script de búsqueda de paquetes*

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

El siguiente comando `rpm -q --changelog rpm` muestra información detallada (actualizaciones, configuración, cambios, etc.) sobre un paquete específico. Este ejemplo proporciona información sobre el paquete `rpm`. No obstante, 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 sólo funciona si el CD 1 está montado en `/media/cdrom`:

```
rpm -qp --changelog /media/cdrom/suse/i586/rpm-4*.rpm
```

La base de datos instalada también permite efectuar verificaciones. Estas 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:

Cuadro 4.9: *Las verificaciones*

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

Para los archivos de configuración aparece como valor adicional la letra `c`, como lo muestra el ejemplo para el archivo `/etc/wgetrc` de `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 en una partición `/usr` de 1 GB, especialmente después de una actualización completa. Si la base de datos parece demasiado gran-

de, 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 base de datos existente. El script `cron` `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_RPMDB_BACKUPS`, cuyo valor por defecto es `5`, pero se puede modificar en `/etc/sysconfig/backup`. Cada copia de seguridad ocupa aproximadamente 3 MB en una partición `/usr` de 1 GB.

4.3.6. Instalar y compilar los paquetes fuente

Todos los paquetes fuente (sources) tienen la extensión `.src.rpm`; estos archivos se llaman "Source-RPMs".

Sugerencia

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 ordinarios. Por esta razón los paquetes fuente no figuran en la base de datos RPM, ya que este sólo anota el software *instalado*.

Sugerencia

Si no hay ninguna configuración personal activada (por ejemplo 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.bz2` o `.tar.gz`, etc.) y para las adaptaciones específicas de las distintas distribuciones (principalmente archivos `.diff` o `.patch`).

`SPECS` para los archivos `.spec`, que controlan el proceso *build* y de este modo actúan como makefiles.

`BUILD` por debajo de este directorio se desempaquetan 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 aquí se guardan los RPM *source* (fuente).

Al instalar con YaST 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 en `SOURCES` y el archivo `.spec` correspondiente en `SPECS`.

Importante

No haga experimentos con RPM y componentes importantes del sistema como pueden ser `glibc`, `rpm`, `sysvinit` etc.: la operatividad de su sistema está en juego.

Importante

Tomemos como ejemplo el paquete `wget.src.rpm`. Después de instalar este paquete con YaST, obtendrá una lista de archivos semejante a esta:

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

Con el comando `rpmbuild -b` ⟨*X*⟩ `/usr/src/packages/SPECS/wget.spec` comienza la compilación. La variable ⟨*X*⟩ es un comodín que puede representar diferentes pasos (vea la salida de `--help` o la documentación de RPM para obtener información adicional). A continuación se explican las opciones brevemente:

`-bp` Prepara las fuentes en el directorio `/usr/src/packages/BUILD`, las desempaqueta y pone los parches.

`-bc` Igual que `-bp`, pero con compilación.

`-bi` Igual que `-bc`, pero con instalación del paquete. Atención: si hay algún paquete que no soporte la característica BuildRoot, es posible que durante la instalación se sobreescriban algunos archivos de configuración importantes.

`-bb` Igual que `-bi`, pero con generación adicional del RPM binario que, en caso de éxito, se encuentra en el directorio `/usr/src/packages/RPMS`.

`-ba` Como `-bb`, pero genera adicionalmente el RPM fuente que se encuentra, en caso de éxito, en el directorio `/usr/src/packages/SRPMS`.

--short-circuit Permite saltarse determinados pasos.

El RPM binario creado ya puede instalarse con `rpm -i` o mejor aún con `rpm -U`. La instalación con `rpm` hace que aparezca en la base de datos RPM.

4.3.7. Compilación de paquetes RPM con build

En el caso de muchos paquetes se corre el riesgo de que se instalen archivos no deseados en el sistema. Para evitarlo se puede emplear el paquete `build`, el cual crea un entorno definido dentro del que se construye 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 crea 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 preferencia de los propios RPMs de cara al resto, saltarse el inicio 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 la página man de `build`.

4.3.8. Herramientas para los archivos RPM y la base de datos RPM

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 de mc. La información de los encabezamientos del archivo `HEADER` se visualiza con (F3). Las teclas del cursor e (Intro) permiten "navegar" por la estructura del archivo y además es posible copiar componentes de un archivo con (F5).

KDE incluye la herramienta kpackage como interfaz para `rpm`. Asimismo un completo gestor de paquetes está disponible en forma de módulo de YaST (ver sección 2.2.1 en la página 40).

Reparación del sistema

Además de numerosos módulos de YaST para la instalación y configuración del sistema, SUSE LINUX dispone también de funciones para reparar el sistema instalado. En este capítulo se describen los distintos métodos y grados de reparación del sistema. El sistema de rescate de SUSE permite al administrador de sistemas experimentado reparar un sistema dañado y proporciona acceso a las particiones.

Para reparar el sistema debe iniciarlo como lo haría en el caso de una nueva instalación, ya que no es seguro asumir que un sistema dañado pueda arrancar por sí mismo y además reparar un sistema en ejecución es bastante complejo. Después de completar los pasos explicados en el capítulo 1 en la página 3, accederá al diálogo para escoger el modo de instalación. Allí debe seleccionarse la opción 'Reparar el sistema instalado'.

Importante

Selección del medio de instalación apropiado

Para que el sistema de reparación funcione correctamente es importante utilizar un medio de instalación que corresponda *exactamente* al sistema instalado.

Importante

A continuación debe seleccionarse el modo de reparación de sistema. Las opciones disponibles son 'Reparación automática', 'Reparación personalizada' y 'Herramientas avanzadas'.

5.1. Reparación automática

Este método es el más indicado para reparar el sistema cuando no se conoce la causa del problema. Después de haberla seleccionado, comienza un análisis exhaustivo del sistema instalado que, debido a la gran cantidad de pruebas y comprobaciones que se realizan, puede llevar un cierto tiempo. El avance de este proceso se refleja en la parte inferior de la pantalla por medio de dos barras. La barra superior muestra el avance de la comprobación parcial que se está ejecutando en ese preciso instante y la barra inferior muestra el avance total. La ventana de control encima de las barras muestra la actividad actual y los resultados de la comprobación (figura **??** en esta página). Se realizan los siguientes grupos de pruebas, si bien cada grupo engloba numerosas comprobaciones subordinadas.

Tablas de particiones de todos los discos duros
Se comprueba la validez y coherencia de las tablas de particiones de todos los discos duros.

Zonas de intercambio Las zonas de intercambio (swap) del sistema instalado se buscan, se comprueban y, en caso necesario, se ofrecen para su activación. Es conveniente confirmar esta oferta de activación para aumentar la velocidad de la reparación del sistema.

Sistemas de archivos Se realiza una comprobación específica para cada sistema de archivos hallado.

Entradas en la tabla `/etc/fstab` Se comprueba si las entradas en este archivo son completas y coherentes. Todas las particiones válidas se montan.

Configuración del cargador de arranque
Se comprueba la integridad y coherencia de la configuración del gestor de arranque (GRUB o LILO). Los dispositivos raíz y de arranque (root y boot) se comprueban y se controla la disponibilidad de los módulos initrd.

Base de datos de paquetes Se comprueba la disponibilidad de todos los paquetes necesarios para una instalación mínima. Una opción adicional es el análisis de los paquetes base. No obstante, esta opción lleva mucho tiempo debido a la gran cantidad de datos que se deben procesar.

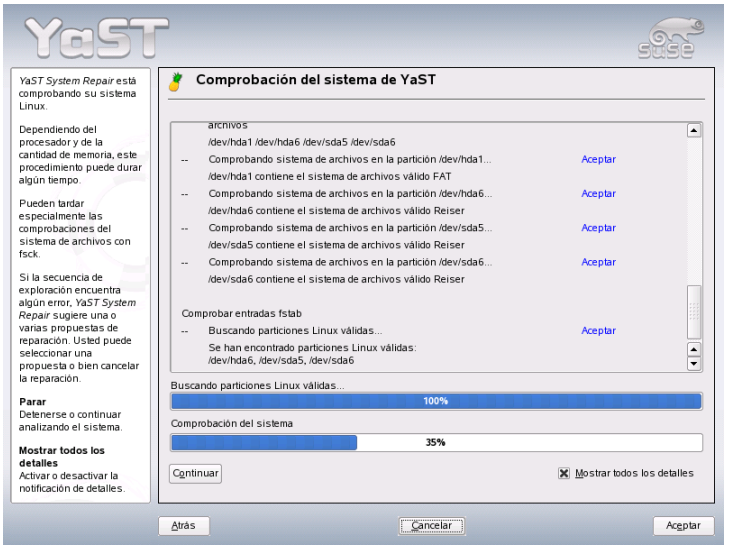

Figura 5.1: *Modo de reparación automática*

Cuando se encuentra un error, el análisis del sistema se detiene y se abre un diálogo mostrando detalles y propuestas para resolver el problema. Por la gran cantidad de pruebas que se efectúan, no nos es posible explicar todos los casos. Lea

atentamente los avisos en pantalla y seleccione una opción de las que se ofrecen. En caso de duda también es posible rechazar el arreglo propuesto. En este caso no se realizarán cambios en el sistema. Nunca se llevará a cabo una reparación automática sin consultar al usuario.

5.2. Reparación personalizada

En la reparación automática explicada en el apartado anterior siempre se realizan todas las pruebas. Esto tiene sentido cuando no se conoce la causa del error. Por otra parte, si ya sabe qué parte del sistema está afectada, puede reducir el número de pruebas que se realizan. Después de haber seleccionado 'Reparación personalizada' aparece una selección de grupos de pruebas en la que todos los grupos están preseleccionados. Esta selección es idéntica a la de la reparación automática. Si ya sabe con seguridad dónde no se encuentra el error, puede desactivar la comprobación correspondiente pulsando sobre la casilla respectiva. Después de pulsar 'Siguiente' se inicia un proceso de comprobación más reducido con un tiempo de ejecución más corto.

No todos los grupos de pruebas pueden aplicarse por separado. Por ejemplo, la comprobación de las entradas de la tabla fstab implica siempre la comprobación de los sistemas de archivos y de las zonas de intercambio. En caso necesario, YaST resuelve estas dependencias seleccionando automáticamente la cantidad mínima de pruebas necesarias.

5.3. Herramientas avanzadas

Si ya dispone de mucha experiencia con SUSE LINUX y tiene una idea concreta de lo que debe repararse en el sistema, puede seleccionar la opción 'Herramientas avanzadas' para aplicar exactamente aquella herramienta que necesita para el arreglo.

Instalar nuevo cargador de arranque Esta opción sirve para iniciar el modulo de YaST para configurar el cargador de arranque. Puede obtener información adicional en la sección ?? en esta página

Iniciar la herramienta de particionamiento
Esta opción le permite iniciar el particionador para expertos de YaST. Puede encontrar más información en el capítulo sección 2.7.5 en la página 73

Reparar sistema de archivos Con esta opción puede comprobar los sistemas de archivos del sistema instalado. En primer lugar aparece una lista con todas las particiones disponibles en la que puede seleccionar aquella que quiere comprobar.

Recuperar particiones perdidas Si las tablas de particiones del sistema están dañadas, esta opción le permite tratar de reconstruirlas. En caso de que el ordenador disponga de varios discos duros, debe seleccionar primero uno de ellos. La comprobación comienza después de pulsar 'OK' y su duración depende del tamaño del disco duro y de la potencia de la máquina.

Importante

Reconstrucción de la tabla de particiones

La reconstrucción de una tabla de particiones no es fácil. YaST intenta detectar las particiones perdidas analizando la zona de datos del disco duro. Si el análisis tiene éxito, la partición se añade a la tabla de particiones recuperada. Lamentablemente esto no funciona en todos los casos.

Importante

Guardar la configuración del sistema a un disquete
Esta opción permite guardar archivos de configuración importantes en un disquete. Si alguno de estos archivos resulta dañado, puede recuperarse desde el disquete.

Verificar el software instalado Esta opción comprueba la coherencia de la base de datos de paquetes así como la disponibilidad de los paquetes más importantes. Si algún paquete instalado estuviera dañado, se puede forzar la reinstalación del mismo desde esta opción.

5.4. El sistema de rescate de SUSE

SUSE LINUX contiene un sistema de rescate que le permite acceder desde fuera a sus particiones Linux en caso de emergencia. Puede cargar el *sistema de rescate* (rescue system) desde un CD, desde la red o desde el servidor FTP de SUSE. El sistema de rescate contiene además una buena selección de programas de ayuda que le permiten solucionar problemas tales como discos duros a los que no se puede acceder o archivos de configuración incorrectos.

Parted (`parted`) también forma parte del sistema de rescate y sirve para modificar el tamaño de las particiones. En caso de necesidad puede ser iniciado manualmente desde el sistema de rescate si no quiere utilizar el redimensionador integrado en YaST. Puede encontrar más información sobre Parted en `http://www.gnu.org/software/parted/`.

5.4.1. Inicio del sistema de rescate

Arranque el sistema al igual que lo haría para la instalación y seleccione 'Rescue System' del menú de arranque. A continuación el sistema de rescate se descomprime y se carga, monta e inicia como un nuevo sistema de archivos raíz en un ramdisk (disco virtual).

5.4.2. Trabajar con el sistema de rescate

Por medio de las teclas (Alt)-(F1) hasta (Alt)-(F3), el sistema de rescate proporciona tres consolas virtuales diferentes. En ellas puede entrar al sistema como usuario `root` sin necesidad de contraseña. Con las teclas (Alt)-(F10) se accede a la consola del sistema para ver los mensajes del kernel y de syslog.

El directorio `/bin` contiene una shell y otras herramientas muy útiles como por ejemplo mount. En `/sbin` dispone de un conjunto de herramientas para archivos y red que sirven por ejemplo para comprobar y arreglar sistemas de archivos (reiserfsck, e2fsck). Aquí se encuentran también los binarios más importantes para la administración del sistema como fdisk, mkfs, mkswap, mount, init y shutdown, así como ifconfig, route y netstat para la operación en red. El directorio `/usr/bin` incluye, además del editor vi, las herramientas grep, find, less y 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 consta de las siguientes particiones Linux especificadas en `/etc/fstab`, tal y como se observa en el ejemplo **??** en esta página.

Ejemplo 5.1: *Ejemplo /etc/fstab*

```
/dev/sdb5       swap        swap        defaults   0   0
/dev/sdb3       /           ext2        defaults   1   1
/dev/sdb6       /usr        ext2        defaults   1   2
```

Aviso

Observe en el siguiente apartado el orden en el que han de montarse los distintos dispositivos.

Aviso

Para tener acceso a todo el sistema hay que montarlo paso a paso mediante `/mnt` con los siguientes comandos:

```
mount /dev/sdb3 /mnt
mount /dev/sdb6 /mnt/usr
```

Ahora tiene acceso a todo el sistema y puede, por ejemplo, corregir errores en archivos de configuración como `/etc/fstab`, `/etc/passwd` o `/etc/inittab`. Estos archivos se encuentran ahora en `/mnt/etc` y no en `/etc`. Es posible recuperar particiones totalmente perdidas, creándolas nuevamente con fdisk. Para ello se recomienda imprimir *previamente* el directorio `/etc/fstab` así como la salida del comando `fdisk -l`.

Reparar sistemas de archivos

Un sistema de archivos dañado es una razón seria para recurrir al sistema de rescate. En principio no es posible reparar un sistema de archivos mientras el sistema está en funcionamiento. En casos graves ni siquiera se puede montar el sistema de archivos raíz y el arranque termina con el mensaje `kernel panic`. En tal caso sólo queda la posibilidad de repararlo desde fuera con un sistema de rescate.

El sistema de rescate de SUSE LINUX contiene las herramientas reiserfsck, e2fsck y dumpe2fs para fines de diagnóstico, con las que se resuelven la mayoría de problemas. Generalmente en casos de emergencia no se puede acceder a la página man de reiserfsck o e2fsck, por lo que se encuentran impresas en el manual en la sección **??** en esta página y sección **??** en esta página respectivamente.

Ejemplo: cuando un sistema de archivos `ext2` no puede montarse debido a un *superbloque no válido*, lo más probable es que `e2fsck` tampoco pueda arreglarlo. La solución consiste en utilizar las copias de seguridad de superbloques que se encuentran cada 8192 bloques (bloque 8193, 16385…) en el sistema de archivos. Para ello utilice el comando `e2fsck -f -b 8193 /dev/damaged_partition`. La opción `-f` fuerza la comprobación del sistema de archivos para evitar que `e2fsck` asuma que todo está en orden por el hecho de haber detectado la copia intacta del superbloque.

Parte II

Sistema

Programas de 32 y 64 bits en entornos de 64 bits

SUSE LINUX está disponible para varias plataformas de 64 bits. Esto no significa necesariamente que todas las aplicaciones hayan sido portadas a 64 bits. SUSE LINUX soporta el uso de aplicaciones de 32 bits en entornos de 64 bits. El presente capítulo le ofrece una visión general sobre la implementación de este soporte en las plataformas de 64 bits de SUSE LINUX. Este capítulo describe cómo se ejecutan las aplicaciones de 32 bits (soporte para tiempo de ejecución) y el modo en que las aplicaciones de 32 bits han de ser compiladas a fin de poder ejecutarlas tanto en entornos de 32 como de 64 bits. Asimismo, incluye información acerca del API del kernel y una explicación sobre cómo pueden ejecutarse las aplicaciones de 32 bits bajo un kernel de 64 bits.

SUSE LINUX para las plataformas de 64 bits AMD64 y EM64T está diseñado de tal forma que las aplicaciones de 32 bits existentes funcionen en entornos de 64 bits sin necesidad de llevar a cabo ninguna configuración. Este soporte le permite seguir utilizando sus aplicaciones de 32 bits preferidas sin tener que esperar a que sean portadas a 64 bits.

6.1. Soporte en tiempo de ejecución

Importante

Conflictos entre las versiones de 32 y 64 bits de una aplicación

Si una aplicación está disponible tanto para 32 como para 64 bits, la instalación paralela de ambas versiones siempre ocasionará problemas. En estos casos es necesario decidirse por una de las dos versiones.

Importante

Todas las aplicaciones requieren una serie de librerías para su correcta ejecución. Lamentablemente los nombres de las librerías de 32 y de 64 bits son idénticos. Por eso hace falta otro mecanismo para distinguirlas.

para mantener la compatibilidad con la versión de 32 bits, las librerías se guardan exactamente en el mismo sitio en el que se guardan en la versión de 32 bits. La versión de 32 bits de la librería `libc.so.6` se encuentra en `/lib/libc.so.6` tanto en los entornos de 32 como de 64 bits.

Todas las librerías y archivos objeto de 64 bits se encuentran en directorios denominados `lib64`. Los archivos objeto de 64 bits que normalmente se encuentran en `/lib`, `/usr/lib` y `/usr/X11R6/lib` se encuentran ahora en `/lib64`, `/usr/lib64` y `/usr/X11R6/lib64`. De esta forma las librerías de 32 bits se pueden guardar en los directorios `/lib`, `/usr/lib` y `/usr/X11R6/lib`. Los nombres de los archivos son idénticos para ambas versiones.

Los subdirectorios de los directorios objeto cuyo contenido binario no dependa del tamaño de la palabra no se mueven. Por ejemplo, los tipos de letra X11 se encuentran como es habitual en `/usr/X11R6/lib/X11/fonts`. Este esquema concuerda con el estándar de Linux LSB (Linux Standards Base) y el FHS (File System Hierarchy Standard).

6.2. Desarrollo de software

La cadena de herramientas de desarrollo Biarch permite generar objetos de 32 y de 64 bits. El estándar es la compilación de objetos de 64 bits. Con opciones especiales es posible generar objetos de 32 bits. En el caso del GCC, la opción correspondiente es `-m32`.

Todos los archivos de cabecera se han de escribir en un formato que no dependa de la arquitectura. Asimismo, las librerías instaladas de 32 y 64 bits deben disponer de una API (Application Programming Interface) que corresponda a los archivos de cabecera instalados. El entorno normal de SUSE ha sido diseñado conforme a este esquema. Si actualiza librerías por su cuenta deberá tener en cuenta estos asuntos.

6.3. Compilación de software en plataformas Biarch

Para compilar en una arquitectura Biarch binarios para la arquitectura contraria, es preciso instalar las librerías correspondientes de la arquitectura adicional. Los paquetes necesarios se denominan `rpmname-32bit`. Además se requieren las cabeceras y librerías que se encuentran en los paquetes `rpmname-devel` así como las librerías de desarrollo de la segunda arquitectura que se encuentran en `rpmname-devel-32bit`.

La mayoría de los programas Open Source utilizan una configuración basada en `autoconf`. La utilización de `autoconf` para la configuración de un programa basado en la segunda arquitectura sólo funciona sobreescribiendo los ajustes normales de compilador y enlazador (efectuados por `autoconf`) con aquellos realizados por el script `configure` con variables de entorno adicionales.

El siguiente ejemplo se refiere a un sistema AMD64 y EM64T con x86 como segunda arquitectura:

1. Haga que `autoconf` utilice el compilador de 32 bits:

   ```
   CC="gcc -m32"
   ```

2. Indique al enlazador que procese objetos de 32 bits:

   ```
   LD="ld -m elf64_i386"
   ```

3. Configure el ensamblador de forma que genere objetos de 32 bits:

   ```
   AS="gcc -c -m32"
   ```

4. Determine que el origen de las librerías para `libtool`, etc. sea `/usr/lib`:

   ```
   LDFLAGS="-L/usr/lib"
   ```

5. Determine que las librerías se copien al subdirectorio `lib`:

   ```
   --libdir=/usr/lib
   ```

6. Defina que se utilicen las librerías X de 32 bits:

   ```
   --x-libraries=/usr/X11R6/lib/
   ```

No se necesitan todas las variables para todos los programas. Adáptelas de acuerdo a sus necesidades.

6.4. Soporte en el kernel

Los kernel de 64 bits para AMD64 y EM64T ofrecen una ABI (Application Binary Interface) de kernel tanto de 32 como de 64 bits. La primera es idéntica a la ABI del kernel correspondiente de 32 bits. Esto significa que las aplicaciones de 32 bits se pueden comunicar con un kernel de 64 bits igual que con uno de 32 bits.

La emulación de 32 bits de consultas de sistema de un kernel de 64 bits no soporta todas las API utilizadas por los programas del sistema. Esto depende de la plataforma. Por este motivo, unas pocas aplicaciones como `lspci` o los programas de gestión de LVM tienen que existir como programas de 64 bits para funcionar correctamente.

Un kernel de 64 bits sólo puede cargar módulos de 64 bits compilados especialmente para ese kernel. Los módulos del kernel de 32 bits no pueden ser utilizados.

Sugerencia

Existen algunas aplicaciones que requieren módulos propios que puedan ser cargados. Si quiere utilizar una aplicación de 32 bits de este tipo en un entorno de 64 bits, contacte con el fabricante del programa y con SUSE para garantizar la disponibilidad de una versión de 64 bits del módulo que pueda cargarse y de la compilación de 32 bits de la API del kernel para este módulo.

Sugerencia

El concepto de arranque de SUSE LINUX

El arranque e inicio de un sistema UNIX es un proceso complejo, ya que están involucrados varios componentes que necesitan interactuar de forma fluida. Este capítulo ofrece una breve introducción al concepto de arranque de SUSE LINUX. También se describe el concepto de niveles de ejecución y la configuración del sistema mediante el empleo de `sysconfig`.

7.1. El proceso de arranque en Linux

El proceso de arranque en Linux consiste en varias etapas, cada una de las cuales está representada por otro componente. La siguiente relación ofrece un breve resumen acerca de cómo se produce el arranque y una descripción sobre los componentes más importantes.

1. **BIOS**

   Después de encender el ordenador, la BIOS (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 se lee la hora, la fecha y los datos de los periféricos más importantes de los valores que están en la CMOS (*CMOS setup*). Una vez que se conoce el primer disco duro y su geometría, la BIOS traspasa el control del sistema al cargador de arranque.

2. **Cargador de arranque**

   Durante este proceso se carga en la memoria el primer sector físico de datos de 512 bytes del primer disco duro y el cargador de arranque (*bootloader*) asume el control al principio de este sector. El orden de las instrucciones ejecutadas a través del cargador de arranque determina el proceso de arranque posterior. Estos primeros 512 bytes en el primer disco duro se denominan en inglés *Master Boot Record* (MBR). El cargador de arranque cede el control sobre el sistema al auténtico sistema operativo, en esta caso, el kernel de Linux. Puede encontrar más información acerca de GRUB, el cargador de arranque de Linux, en el capítulo **??** en esta página.

3. **Kernel e initrd**

   El cargador de arranque almacena tanto el kernel como un disco RAM inicial (initial RAM disk o initrd) en memoria a fin de poder traspasar el control al sistema. El kernel de Linux incluye una opción para poder guardar un sistema de archivos reducido en un disco RAM, pudiendo ejecutar así programas antes de montar el sistema de archivos real. El kernel descomprime a continuación initrd y monta un sistema de archivos raíz temporal. El contenido de initrd es un sistema Linux mínimo que contiene un ejecutable llamado linuxrc. linuxrc carga unos módulos especiales del kernel que permiten acceder al sistema de archivos raíz real. El kernel libera la memoria ocupada por initrd y arranca init después de que linuxrc haya finalizado correctamente, Puede encontrar más información acerca de initrd en la sección **??** en esta página.

4. **linuxrc**

   Este programa ejecuta todas las acciones necesarias para montar el sistema de archivos raíz. Tan pronto como el sistema de archivos raíz real ha sido montado con éxito, linuxrc se detiene y el kernel inicia el programa init. Puede encontrar más información a este respecto en la sección **??** en esta página.

5. **init**

   init gestiona el arranque en sí del sistema a través de diferentes niveles de funcionalidad. init está descrito en la sección **??** en esta página.

7.1.1. initrd

initrd consiste en un sistema de archivos reducido (normalmente comprimido) que carga el kernel en un disco RAM inicial y que posteriormente es montado como un sistema de archivos raíz temporal. Proporciona un entorno Linux mínimo que permite la ejecución de programas antes de que el sistema de archivos raíz real pueda ser montado. Este entorno mínimo de Linux es cargado en la memoria por rutinas BIOS y su único requisito de hardware es contar con suficiente memoria. initrd siempre tiene que proporcionar un ejecutable llamado linuxrc que debe procesarse sin errores.

Antes de que el sistema de archivos raíz real sea montado y que el sistema operativo en sí pueda ser iniciado, el kernel necesita conocer los controladores que se requieren para acceder al dispositivo que alberga el sistema de archivos raíz. Estos controladores pueden ser especiales para un tipo específico de disco duro o incluso de red para permitir el acceso a un sistema de archivos de red (consulte en esta página). El kernel ha de contener también el código necesario para leer el sistema de archivos de initrd. linuxrc puede cargar los módulos necesarios para el sistema de archivos raíz.

Cree un `initrd` mediante el script `mkinitrd`. En SUSE LINUX, los módulos que han de cargarse están especificados por la variable `INITRD_MODULES` ubicada en `/etc/sysconfig/kernel`. Tras la instalación, esta variable adquiere automáticamente el valor correcto (el linuxrc de la instalación guarda qué modulos han sido cargados). Los módulos son cargados en el mismo orden que se indica en `INITRD_MODULES`. Este hecho es especialmente importante si se emplean varios controladores SCSI, ya que de otro modo los nombres de los discos duros podrían cambiar. En sentido estricto, debería ser suficiente con cargar simplemente los controladores necesarios para acceder al sistema de archivos raíz.

Sin embargo, initrd lee todos los controladores SCSI requeridos para la instalación ya que sería problemático realizar este proceso posteriormente.

Importante

Actualización de initrd

El cargador de arranque lee initrd del mismo modo que el kernel. No es necesario reinstalar GRUB tras una actualización de initrd ya que GRUB busca el archivo correcto en el directorio durante el arranque.

Importante

7.1.2. linuxrc

El fin principal de linuxrc es preparar el montaje de y el acceso al sistema de archivos raíz real. Dependiendo de la configuración del sistema, linuxrc es responsable de las siguientes tareas.

Cargar los módulos del kernel Según la configuración del hardware, es necesario disponer de controladores especiales para acceder a ciertos componentes de hardware presentes en el equipo (principalmente, el disco duro). Para poder acceder al sistema de archivos raíz final, el kernel necesita cargar los controladores de sistema de archivo apropiados.

Gestionar RAID y LVM Si ha establecido que el equipo albergue el sistema de archivos raíz bajo RAID o LVM, linuxrc configura LVM o RAID para permitir el acceso posterior al sistema de archivos raíz. Puede encontrar información adicional acerca de RAID en la sección **??** en esta página. Para LVM, consulte la sección 3.6 en la página 100.

Gestionar la configuración de red Si ha configurado el sistema para utilizar un sistema de archivos raíz montado en red (a través de NFS), linuxrc debe asegurarse de que se encuentren cargados los controladores de red y de que éstos permiten el acceso al sistema de archivos raíz.

Cuando linuxrc es ejecutado durante el arranque inicial como parte del proceso de instalación, sus tareas difieren de las mencionadas anteriormente:

Localizar el medio de instalación En el momento de iniciar el proceso de instalación, el equipo carga un kernel especial desde el medio de instalación

y un initrd especial con el instalador de YaST. El instalador de YaST, que se ejecuta en el sistema de archivos del disco RAM, necesita conocer la ubicación real del medio de instalación a fin de poder acceder a él e instalar el sistema operativo.

Iniciar el reconocimiento de hardware y cargar los módulos del kernel apropiados Modules
Como se ha mencionado en la sección **??** en esta página, el proceso de arranque comienza con un conjunto mínimo de controladores que pueden ser empleados con la mayoría de configuraciones de hardware. linuxrc ejecuta la identificación inicial del hardware a fin de determinar qué controladores son necesarios para acceder al hardware de su sistema. Esta información es guardada posteriormente en `INITRD_MODULES` ubicado en `/etc/sysconfig/kernel` a fin de permitir los arranques de sistema posteriores. Durante el proceso de instalación, linuxrc carga este conjunto de módulos.

Cargar el sistema de instalación o el de rescate
Tan pronto como el hardware ha sido correctamente reconocido y los controladores correspondientes han sido cargados, linuxrc ejecuta el sistema de instalación, el cual contiene el verdadero instalador YaST o el sistema de rescate.

Arrancar YaST Finalmente, linuxrc inicia YaST, el cual ejecuta la instalación de paquetes y la configuración del sistema.

7.1.3. Información adicional

Si desea obtener más información respecto a los temas tratados, puede consultar `/usr/src/linux/Documentation/ramdisk.txt`, `/usr/src/linux/Documentation/initrd.txt` y las páginas de manual initrd(4) y mkinitrd(8).

7.2. 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 o de los hijos de este. 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 (runlevel) (se comenta con más detalle en la sección **??** 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 reunen 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.

7.3. Los niveles de ejecución — runlevels

Bajo Linux existen diferentes *runlevels* (niveles de ejecución), que definen cómo se inicia el sistema y qué servicios deben estar disponibles en el sistema activo. 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 **??** en esta página). Alternativamente se puede introducir el nivel de ejecución requerido en el proceso de arranque (por ejemplo 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 (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 sin necesidad de emplear X. Si desea activar un entorno gráfico como GNOME, KDE, etc., ejecute el comando `init 5`. Con `init 0` o `shutdown -h now` se puede parar el sistema y con `init 6` o `shutdown -r now` reiniciarlo.

Importante

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.

Importante

Cuadro 7.1: *Lista de los niveles de ejecución disponibles en Linux*

Nivel de ejecución	Significado
0	Parada de sistema (system halt)
S	Modo monousuario (single user mode) desde el prompt de arranque
1	Modo monousuario (single user mode)
2	Modo multiusuario local sin red remota (local multiuser without remote network) (ej. NFS)
3	Modo multiusuario completo con red (full multiuser with network)
4	Libre (not used)
5	Modo multiusuario completo con red y KDM (estándar), GDM o XDM (full multiuser with network and xdm)
6	Reiniciar el sistema (system reboot)

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 el valor es `3`, es necesario configurar el sistema X Window de forma correcta, tal y como se describe en el capítulo **??** en esta página, antes de poder cambiar el nivel de ejecución a `5`. Una vez realizado este paso, ha de comprobar si el sistema funciona de la forma deseada

mediante la ejecución del comando `init 5`. Si el sistema se comporta del modo esperado, puede utilizar YaST para establecer el nivel de ejecución por defecto en 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. A continuación, asigne permiso de escritura al sistema de archivos raíz con el comando `mount -o remount,rw /` y sustituya `/etc/inittab` por la copia de seguridad por medio del comando `cp`. Para evitar errores en el sistema de archivos, vuelva a cambiar el sistema de archivos raíz a sólo lectura antes de reiniciar el sistema: `mount -o remount,ro /`.

Aviso

7.4. 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 este, 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.

- Por último se llama a los scripts de arranque del nuevo nivel de ejecución. Estos 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 (por ejemplo ejecuta un getty en otra interfaz).

7.5. Los scripts de inicio

Los scripts bajo `/etc/init.d` se dividen en dos categorías:

Scripts ejecutados directamente por init
: Esto sólo sucede durante el arranque o en caso de un apagado instantáneo (en caso de un corte del suministro eléctrico o por pulsar el usuario la combinación de teclas Ctrl-Alt-Supr). La ejecución de estos scripts se define en `/etc/inittab`.

Scripts ejecutados directamente 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, estos 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 **??** en esta página. Los scripts ejecutados directamente por init carecen de estos enlaces. Dichos scripts se ejecutan cuando es necesario independientemente del nivel de ejecución.

Cuadro 7.2: *Resumen de las opciones de los scripts de inicio*

Opción	Significado
`start`	Iniciar el servicio
`stop`	Parar el servicio
`restart`	Con el servicio en ejecución, pararlo y reiniciarlo; en caso contrario, iniciarlo
`reload`	Leer la configuración del servicio nuevamente sin parada y reinicio del servicio
`force-reload`	Leer nuevamente la configuración del servicio si este lo soporta; en caso contrario igual que restart
`status`	Mostrar estado actual

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 `man 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 `pts`, se arranca el blogd (boot logging daemon) 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 subscripts). 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 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.

`\mbox{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.

7.5.1. 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(8), init.d(7), e insserv(8). Las páginas del manual de startproc(8) y killproc(8) 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 la sección ?? en esta página.

Aviso

Si desea crear un script init para un programa o servicio (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:

Ejemplo 7.1: *Bloque INIT INFO mínimo*

```
### BEGIN INIT INFO
# Provides:          FOO
# Required-Start:    $syslog $remote_fs
# Required-Stop:     $syslog $remote_fs
# Default-Start:     3 5
# Default-Stop:      0 1 2 6
# Description:       Start FOO to allow XY and provide YZ
### END INIT INFO
```

En la primera línea 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 los directorios de niveles de ejecución (`/etc/init.d/rc?.d/`) a los scripts correspondientes en `/etc/init.d/`. insserv analiza automáticamente los datos introducidos en la cabecera `INIT INFO` y guarda los enlaces para los scripts de arranque y parada en los directorios de niveles de ejecución respectivos (`/etc/init.d/rc?.d/`). 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 **??** en esta página .

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.

No defina estos enlaces manualmente. El bloque `INFO` contiene algún error, puede haber problemas cuando `insserv` se ejecute posteriormente para otro servicio.

7.6. Servicios del sistema (niveles de ejecución)

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.

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 o "initdefault". Este "nivel

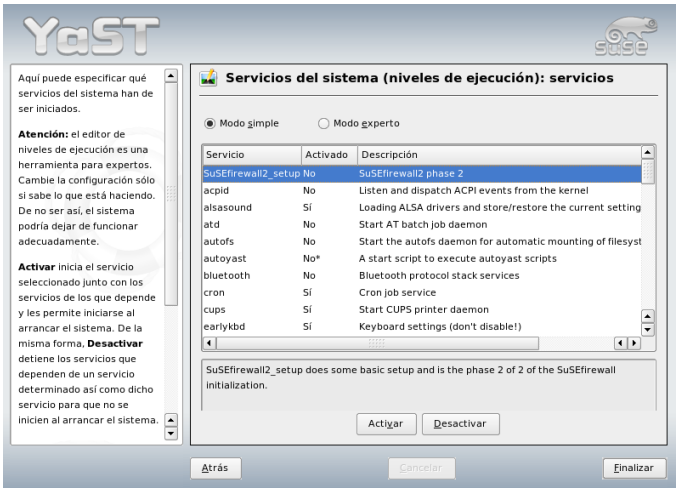

Figura 7.1: *Servicios del sistema (niveles de ejecución)*

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 X). Otro nivel adecuado sería por ejemplo el número 3 (modo multiusuario completo con red).

YaST le permite definir en esta máscara otro nivel de ejecución predeterminado, ver tabla ?? en esta página. 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 ('B' '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.

Con 'Iniciar/parar/actualizar' puede activar o desactivar un determinado servicio. 'Actualizar estado' comprueba el estado actual en caso de que esto no se produzca automáticamente. Mediante 'Aplicar/restaurar' puede decidir si desea trabajar con la configuración modificada por usted o bien recuperar la configuración predeterminada (el estado posterior a la instalación del sistema). 'Terminar' guarda la configuración de sistema.

Aviso

Editar las configuración de los niveles de ejecución

La configuración defectuosa de los servicios del sistema y de los niveles de ejecución pueden provocar un fallo general del sistema. Antes de modificar la configuración, infórmese de las posibles consecuencias a fin de proteger el funcionamiento del sistema.

Aviso

7.7. SuSEconfig y /etc/sysconfig

Gran parte de la configuración de SUSE LINUX se puede realizar mediante los archivos de configuración en `/etc/sysconfig`. 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 por ejemplo, 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 este 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:

1. Ejecutar el comando `init 1` para cambiar el sistema al nivel de ejecución 1 ”single user mode”.

2. 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 sección **??** en esta página.

   Aviso

   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 (por ejemplo `KEYTABLE=""`) y entrecomille también los parámetros que contengan espacios. Esto no es necesario para las variables formadas por una única palabra.

   Aviso

3. Ejecutar SuSEconfig para realizar los cambios en los diferentes archivos de configuración. Esto ocurre automáticamente si las modificaciones se realizan con YaST.

4. 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 (por ejemplo 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.

Sugerencia

Manejo de configuración automática del sistema

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 instalación, debe dar el valor `yes` a la variable `ENABLE_SUSECONFIG`. También es posible deshabilitar la configuración automática selectivamente.

Sugerencia

7.8. El editor sysconfig de YaST

En el directorio `/etc/sysconfig` se encuentran los archivos que contienen las configuraciones más importantes de SUSE LINUX. 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.

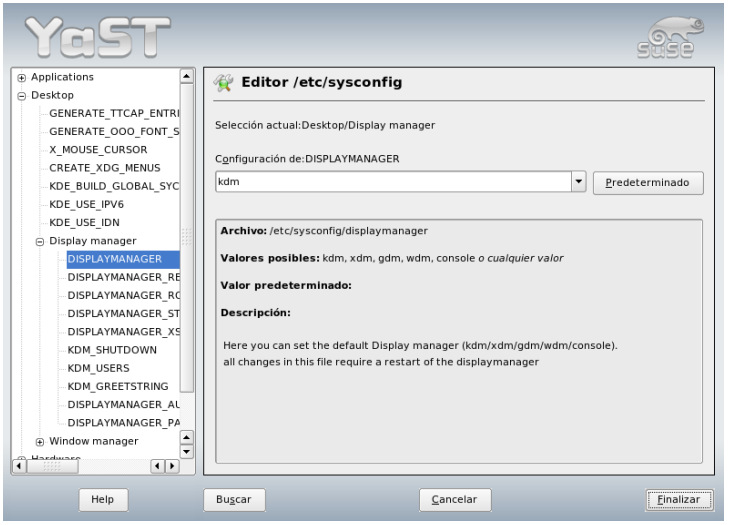

Figura 7.2: *YaST: Configuración con el editor sysconfig*

El cargador de arranque

Este capítulo describe cómo configurar GRUB, el cargador de arranque utilizado actualmente en SUSE LINUX. A efectos de configuración, un módulo de YaST le permite definir todas las opciones necesarias. Si no está familiarizado con el concepto de arranque de Linux, le recomendamos leer los siguientes párrafos para adquirir algunas nociones teóricas. Al final del capítulo se presentan algunos de los problemas más frecuentes que pueden ocurrir durante el arranque con GRUB acompañados de sus respectivas soluciones.

Este capítulo se concentra principalmente en la gestión del arranque y la configuracíón del cargador de arranque GRUB. El proceso de arranque como tal se describe en el capítulo ?? en esta página. Un cargador de arranque constituye la interfaz entre el equipo (BIOS) y el sistema operativo (SUSE LINUX). La configuración del cargador de arranque determina el sistema operativo que va a iniciarse así como sus opciones.

Los siguientes términos se usan con frecuencia en este capítulo, por lo que se explican brevemente

Master Boot Record La estructura del MBR está definida por una convención independiente del sistema operativo. Los primeros 446 bytes están reservados para código de programas. Los 64 bytes siguientes ofrecen espacio para una tabla de particiones de hasta 4 entradas (vea a este respecto la sección Tipos de particiones en la página 11). La tabla de particiones contiene información requerida por el sistema operativo sobre la distribución del disco duro y el tipo de sistema de archivos. Sin la tabla de particiones, al sistema operativo le sería prácticamente imposible utilizar el disco duro. Los últimos dos 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.

Sector de arranque Los sectores de arranque son los primeros que se encuentran en 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 esa partición. Esto se aplica a los sectores de arranque de particiones DOS, Windows u OS/2, que además 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 dos bytes la misma "cifra mágica" que el MBR (AA55).

8.1. Gestión de arranque

El concepto de "gestión de arranque" más simple que uno se puede imaginar es el de un ordenador con un solo sistema operativo como en el caso explicado en

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

Arrancar sistemas adicionales desde medios externos
Los sistemas operativos se cargan del disco. Alternativamente, los gestores de arranque instalados en medios externos (disquete, CD, soporte de memoria USB), permiten iniciar sistemas operativos adicionales. No obstante, debido a que GRUB puede cargar el resto de sistemas operativos, la presencia de un cargador de arranque externo resulta innecesaria.

Instalación de un gestor de arranque en el MBR
Un gestor de arranque (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 elegido resulte adecuado para todos los sistemas operativos instalados. El gestor de arranque de SUSE LINUX, GRUB, permite arrancar todos los sistemas operativos de uso extendido. Por defecto, SUSE LINUX instala el gestor de arranque deseado en el MBR para que esta opción de configuración no se modifique durante la instalación.

8.2. Cómo determinar el cargador de arranque

En SUSE LINUX se utiliza normalmente el cargador de arranque GRUB. No obstante, en unos pocos casos excepcionales así como con configuraciones especiales de hardware o software, es necesario emplear el cargador de arranque alternativo LILO. Si actualiza el sistema desde una versión anterior de SUSE LINUX en la que se utilizaba LILO, se volverá a instalar este cargador de arranque. En el caso de una nueva instalación se empleará GRUB a no ser que la partición raíz esté instalada en los siguientes sistemas Raid:

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

Para obtener información sobre la instalación y configuración de LILO, introduzca el término de búsqueda *LILO* en la base de datos de soporte.

8.3. Arrancar con GRUB

GRUB (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.

stage2 puede acceder directamente al sistema de archivos. Actualmente se soportan Ext2, Ext3, ReiserFS, Minix y el sistema DOS FAT utilizado por Windows. Con algunas limitaciones, también se soporta JFS XFS así como UFS/FFS, el sistema de archivos de los sistemas BSD. Desde la versión 0.95, GRUB es capaz de arrancar desde un CD o DVD con un sistema de archivos estándar conforme a ISO 9660 de acuerdo a la especificación "El Torito". GRUB puede acceder a los sistemas de archivos en los dispositivos de disco BIOS soportados (disquetes o unidades de CD, DVD o discos duros detectados por la BIOS) antes de arrancar, por lo que los cambios en el archivo de configuración de GRUB (`menu.lst`) 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.

Para la configuración de GRUB son necesarios tres archivos que se describen a continuación:

`/boot/grub/menu.lst` Este archivo contiene la información relativa a las particiones y a los sistemas operativos que pueden arrancarse con GRUB. Sin estos datos no sería posible ceder el control del sistema al sistema operativo.

`/boot/grub/device.map` Este archivo "traduce" los nombres de dispositivo de la notación GRUB/BIOS a la nomenclatura Linux.

`/etc/grub.conf` Este archivo contiene los parámetros y opciones requeridos por la shell de GRUB para instalar el cargador de arranque correctamente.

GRUB puede manejarse de distintas formas. Las entradas de arranque de la configuración existente se seleccionan a través de un menú gráfico (splash screen). La configuración se carga del archivo `menu.lst`.

GRUB puede modificar todos los parámetros de arranque *antes* del proceso de inicio, lo que permite resolver un error cometido al editar el archivo del menú. Asimismo, los comandos de arranque pueden introducirse de forma interactiva por medio de una especie de prompt (vea la sección Modificar las entradas de menú durante el proceso de arranque en esta página). GRUB le permite averiguar la situación del kernel y de `initrd` antes de arrancar, posibilitando el arranque de un sistema operativo instalado para el que todavía no existe ninguna entrada en la configuración del cargador de arranque.

Finalmente, la *shell de GRUB* proporciona una emulación de GRUB en el sistema instalado. Puede utilizar esta shell para instalar GRUB o para probar una nueva configuración antes de aplicarla (véase también la sección **??** en esta página).

8.3.1. 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 todas las 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. Si desea realizar cambios en la configuración de GRUB, utilice el módulo del cargador de arranque de YaST (sección ?? en esta página).

Este archivo de menú contiene comandos de sintaxis 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 = 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 GRUB *anotación por bloque* (block-notation), por ejemplo:

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

Los nombres de dispositivo que se encuentran en GRUB se explican en la sección 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 (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 esta página.

Convención de nombres para discos duros y particiones

Para denominar a los discos duros y particiones, GRUB utiliza convenciones distintas a las ya conocidas de los dispositivos Linux normales. 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`.

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`:

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

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.

El problema en GRUB es que no resulta fácil realizar la correspondencia entre los nombres de dispositivo Linux y los nombres de dispositivo de la BIOS. GRUB utiliza un algoritmo para generar esta correspondencia y la guarda en un archivo (`device.map`) que puede ser editado. Puede obtener información adicional sobre el archivo `device.map` en la sección **??** en esta página.

Una ruta completa de GRUB consta de un nombre de dispositivo que se escribe entre paréntesis y 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/blue 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 en el menú de GRUB al que accede tras 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. Las secciones para cada sistema operativo comienzan con la entrada `title`.

- La primera entrada (`title linux`) se encarga del arranque de SUSE LINUX. El kernel (`vmlinuz`) 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 de edición de GRUB (consulte la sección Modificar las entradas de menú durante el proceso de arranque en esta página)

Modificar las entradas de menú durante el proceso de arranque

Por medio de las teclas de cursor puede seleccionar en el menú gráfico de GRUB el sistema operativo que desea arrancar. Si selecciona un sistema Linux, puede añadir sus propios parámetros en el cursor de arranque. Si pulsa (Esc) para salir de la pantalla de bienvenida e introduce a continuación (e) (edit), 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.

Importante

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.

Importante

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 de (b). Un texto de ayuda en la parte inferior de la pantalla le informa sobre el resto de opciones disponibles.

Si desea guardar de forma permanente las opciones de arranque modificadas y pasárselas al kernel, abra el archivo `menu.lst` como usuario `root` e introduzca

los parámetros adicionales del kernel en la línea existente separándolos entre sí con espacios:

```
title linux
kernel (hd0,0)/vmlinuz root=/dev/hda3 <párametros 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 se añade a una línea ya existente separándolo mediante un espacio.

Selección del kernel de arranque mediante comodines

Sobre todo cuando se desarrollan o utilizan kernels personalizados, es necesario modificar las entradas de `menu.lst` o editar la línea de comandos para reflejar los nombres actuales del kernel y del archivo initrd. Con el fin de simplificar este proceso, se recomienda el uso de *comodines* para actualizar dinámicamente la lista de kernels de GRUB. Todas las imágenes del kernel que coinciden con un patrón específico se añaden a la lista de imágenes arrancables. Tenga en cuenta que nuestro servicio de soporte no presta asistencia para esta función.

Si desea activar la opción de comodines, introduzca una entrada de menú adicional en `menu.lst`. Para que esta opción pueda aplicarse, todas las imágenes del kernel e initrd deben tener un nombre base común y un identificador que asocie el kernel con el initrd correspondiente. Vea por ejemplo la siguiente configuración:

```
initrd-default
initrd-test
vmlinuz-default
vmlinuz-test
```

En este caso puede añadir dos imágenes de arranque en una configuración de GRUB. Para obtener las entradas de menú `linux-default` y `linux-test`, debe añadir la siguiente entrada a `menu.lst`:

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

En este ejemplo, GRUB examina la partición (hd0,4) en busca de entradas que coincidan con el comodín. Esas entradas se utilizan para generar nuevas entradas de menú de GRUB. En el ejemplo anterior, GRUB actuaría como si `menu.lst` incluyera las siguientes entradas:

```
title linux-default
   wildcard (hd0,4)/vmlinuz-default
   kernel (hd0,4)/vmlinuz-default root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd-default
title linux-test
   wildcard (hd0,4)/vmlinuz-test
   kernel (hd0,4)/vmlinuz-test root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd-test
```

Los problemas con esta configuración pueden surgir cuando los nombres de archivo no se usan de forma consecuente o falta alguno de los archivos extendidos (por ejemplo una imagen initrd).

8.3.2. 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 de la BIOS sobre el orden de arranque. 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/sda
```

Debido a que el orden de IDE, SCSI y otros discos duros depende de diversos factores y a que Linux no es capaz de detectar dicha correspondencia, existe la posibilidad de determinar el orden manualmente en el archivo `device.map`. Si al arrancar el sistema se producen problemas, compruebe si el orden de arranque en el archivo coincide con el orden especificado en la BIOS. En caso necesario, modifíquelo durante el arranque con ayuda de la shell de GRUB descrita en la sección ?? en esta página. Una vez que el sistema Linux ha arrancado, puede modificar el

archivo `device.map` de forma permanente mediante el módulo del cargador de arranque de YaST o cualquier otro editor.

Tras modificar el archivo `device.map` manualmente, ejecute el siguiente comando para reinstalar GRUB. Al hacerlo, el archivo `device.map` se cargará de nuevo y los comandos incluidos en `grub.conf` se ejecutarán:

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

8.3.3. 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.

8.3.4. La shell de 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 de 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 de GRUB cuando Linux está cargado.

Los comandos `setup` e `install` están disponibles también *durante* el proceso de arranque sin necesidad de que Linux se esté ejecutando. De este modo se simplifica la recuperación de un sistema defectuoso (que no puede arrancarse), ya que el archivo de configuración dañado del cargador de arranque puede evitarse mediante la introducción manual de parámetros. La introducción manual de parámetros durante el arranque resulta también muy adecuada para probar nuevas configuraciones cuando el sistema nativo no debe dañarse bajo ningún concepto. Introduzca simplemente el comando de configuración experimental con una sintaxis parecida a la del archivo `menu.lst` y pruebe la funcionalidad de esta entrada sin modificar el archivo de configuración actual y por tanto sin riesgo para la capacidad de arranque del sistema. Si por ejemplo desea probar un nuevo kernel, introduzca el comando `kernel` incluyendo la ruta al kernel alternativo. En caso de que el proceso de arranque falle, vuelva a utilizar para el próximo arranque el archivo `menu.lst` intacto. Por supuesto, la interfaz de la línea de comandos también resulta muy adecuada para poder arrancar el sistema a pesar de un archivo `menu.lst` defectuoso: simplemente introduzca el parámetro corregido en la línea de comandos. Para que el sistema pueda arrancarse de forma permanente, ha de añadir este parámetro a `menu.lst` mientras el sistema está activo.

El algoritmo de correspondencia de los nombres de dispositivo GRUB y Linux se activa sólo cuando la shell GRUB se ejecuta como programa Linux (para lo que se emplea el comando `grub` como se describe en la sección ?? en esta página). El programa lee a tal efecto el archivo `device.map`. Puede obtener información adicional en la sección ?? en esta página.

8.3.5. 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`:

1. Introduzca el comando `grub` en el símbolo de espera de órdenes de `root`.
2. Codifique la contraseña en la shell de GRUB:

```
grub> md5crypt
Password: ****
Encrypted: $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

3. 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/$JOYcdxIn7CJk9xShzzJVw/
   ```

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

4. 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).

Importante

Contraseña de arranque y pantalla de bienvenida

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

Importante

8.4. Configuración del cargador de arranque con YaST

El modo más sencillo de configurar el cargador de arranque es mediante el módulo de YaST. Active el módulo 'Configuración del cargador de arranque' del menú 'Sistema' en el centro de control de YaST. La ventana que se abre a continuación le muestra la configuración actual del cargador de arranque en el sistema y le permite modificarla (figura **??** en esta página).

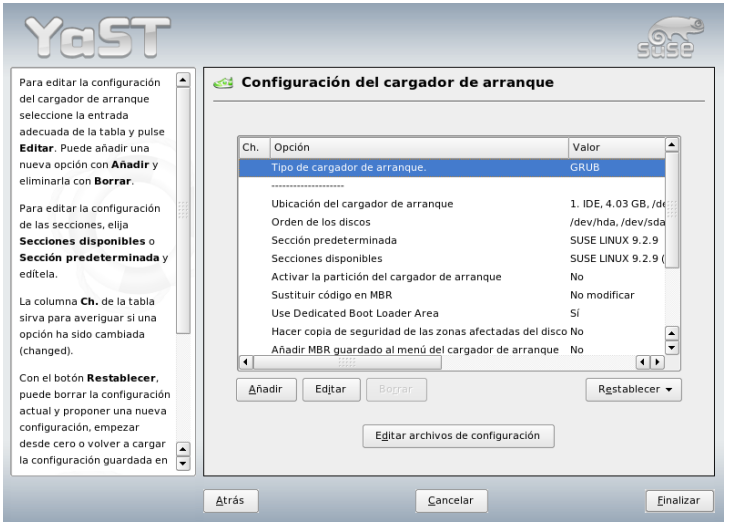

Figura 8.1: *Configuración del cargador de arranque con YaST*

8.4.1. La ventana principal

La ventana de configuración de fondo blanco está dividida en tres columnas: a la izquierda, en 'Ch.', aparecen seleccionadas las opciones modificadas que se ejecutan en la columna central. Los valores actuales se encuentran en la columna de la derecha. Para añadir una opción nueva, pulse el botón 'Añadir'. Si por el contrario sólo quiere cambiar el valor de una opción, selecciónela con el ratón y

después pulse 'Cambiar'. Si no quiere utilizar una opción existente, selecciónela y pulse 'Eliminar'. A la derecha de la ventana de configuración se encuentra un cuadro de selección titulado 'Restablecer' que contiene las siguientes opciones:

Proponer nueva configuración El sistema crea una propuesta nueva de configuración. Si se encuentran versiones anteriores de Linux u otros sistemas operativos en otras particiones, serán integrados en el menú de arranque. En tal caso es posible seleccionar entre el arranque directo de Linux o el arranque a través del antiguo cargador de arranque. Esto último significa tener un segundo menú de inicio.

Iniciar nueva configuración desde cero
Con esta opción usted crea la configuración por sí mismo sin que medie ayuda ninguna en forma de propuestas.

Cargar la configuración guardada en el disco
Si ya ha realizado algunos cambios y no está satisfecho con el resultado, esta opción le permite recargar la configuración guardada en último lugar. De esta forma puede volver al estado de configuración existente en el sistema.

Proponer y fusionar con los menús existentes de GRUB
El menú se compondrá de una entrada para el nuevo SUSE LINUX, una entrada para el otro sistema operativo y todas las entradas de los menús de arranque anteriores. Esto es válido cuando hay otro sistema operativo o una versión anterior de Linux instalados en otras particiones. Este proceso puede llevar algo de tiempo. Con LILO esta opción no existe.

Restablecer MBR del disco duro Con esta opción se recupera el MBR que se encuentra en el disco duro.

Pulse el botón 'Editar archivos de configuración' para acceder a los archivos de configuración en un editor. Seleccione el archivo dentro del campo de selección para editarlo directamente. Al pulsar 'OK' los cambios se graban. Use 'Cancelar' para salir de la configuración sin grabar la configuración del cargador de arranque y 'Atrás' para volver a la ventana principal.

8.4.2. Opciones de configuración del cargador de arranque

La configuración guiada por YaST resulta más fácil que editar los archivos directamente. Seleccione una opción con el ratón y pulse 'Cambiar'. Aparecerá una ventana de diálogo en la que puede realizar ajustes individuales. Al pulsar en

'Aceptar' confirma las modificaciones y vuelve a la ventana de diálogo principal en la que puede editar otras opciones. Estas opciones varían en función del cargador de arranque. A continuación le mostramos algunas opciones de GRUB:

Tipo de cargador de arranque Esta opción le permite cambiar de GRUB a LILO y viceversa. Al seleccionarla accederá a otro diálogo en el que puede especificar el tipo de cambio. Puede transformar la configuración de GRUB en una configuración similar de LILO, si bien podría perder información en caso de no existir equivalencias. Además puede crear una configuración completamente nueva o aceptar una propuesta que podrá editar y modificar.

Si activa la configuración del cargador de arranque mientras el sistema está en funcionamiento, es posible seguir leyendo la configuración desde el disco duro. Si decide volver a utilizar un cargador de arranque ya configurado, puede cargar de nuevo la configuración por medio de la última opción. Todo esto sólo es posible mientras permanezca en el módulo del cargador de arranque.

Ubicación del cargador de arranque En esta ventana de diálogo se especifica dónde se debe instalar el cargador de arranque: en el Master Boot Record (MBR), en el sector de arranque de la partición de arranque (si esta existe), en el sector de arranque de la partición root o en un disquete. Escoja la opción 'Otros' si quiere que se instale en otro sector de arranque.

Orden de los discos Si dispone de dos o más discos duros en su equipo, indique aquí la secuencia correspondiente a la configuración de la BIOS.

Sección predeterminada En esta opción se especifica el kernel o sistema operativo que debe arrancar por defecto en caso de que no se realice ninguna selección en el menú de arranque. Una vez pasado el tiempo de espera se arrancará el sistema predeterminado. Haga clic en esta opción y a continuación pulse el botón 'Editar' para ver todas las entradas del menú de arranque. Seleccione la entrada correspondiente y pulse el botón 'Fijar como estándar'. Asimismo, puede editar una entrada pulsando en 'Cambiar'.

Secciones disponibles Con esta opción puede ver en la ventana principal qué entradas existen en el menú. Si selecciona esta opción y pulsa en 'Cambiar', accederá al mismo diálogo que en 'Sección predeterminada'.

Activar la partición del cargador de arranque
En esta opción se puede activar la partición en la que se ha instalado el sector de arranque del cargador de arranque, independientemente de la

partición en que se encuentre el directorio `/boot` o `/` (root) con los archivos del cargador de arranque.

Sustituir código en MBR Si previamente había instalado GRUB directamente en el MBR o lo instala en un disco duro completamente nuevo y ya no desea instalar GRUB en el MBR, esta opción le permite restaurar el código de arranque genérico en el MBR y sobreescribir GRUB.

Hacer copia de seguridad de archivos y particiones
Se hará una copia de seguridad de las zonas del disco duro que hayan sido modificadas.

Añadir MBR guardado al menú del cargador de arranque
El MBR guardado se añade al menú del cargador de arranque.

Una de las opciones más interesantes de la sección inferior es la del 'Time-out', que determina el tiempo de espera antes de iniciar el sistema. El botón'Añadir' permite establecer opciones adicionales, pero para ello hace falta un buen conocimiento de la materia. Para obtener información adicional sobre las opciones posibles, consulte las páginas del manual correspondientes (`man grub`, `man lilo`) y la documentación en línea `http://www.gnu.org/software/grub/manual/`.

8.5. Desinstalar el cargador de arranque de Linux

YaST se encarga de desinstalar el cargador de arranque de Linux y de devolver el MBR al estado anterior a la instalación de Linux. Durante la instalación, YaST crea automáticamente una copia de seguridad del MBRs y la instala a petición del usuario para sobreescribir GRUB.

Para desinstalar GRUB, inicie el módulo del cargador de arranque de YaST ('Sistema' → 'Configuración del cargador de arranque'). Seleccione en el primer diálogo 'Restablecer' → 'Restablecer MBR del disco duro' y salga del diálogo con 'Finalizar'. A continuación, GRUB será sobreescrito en el MBR con los datos del MBR original.

8.6. Crear un CD de arranque

En caso de que tenga problemas para arrancar el sistema instalado con un gestor de arranque o bien no quiera o pueda instalar el cargador de arranque en el MBR de su ordenador o en un disquete, puede crear un CD de arranque en el que haya grabado los archivos de inicio de Linux. Para ello es necesario que el ordenador disponga de una grabadora de CDs configurada.

Para crear un CD-ROM arrancable con GRUB, tan solo necesita una forma especial de *stage2* llamada `stage2_eltorito` y, de manera opcional, un archivo `menu.lst` personalizado. Los archivos `stage1` y `stage2` clásicos no son necesarios.

Cree un directorio en el que fabricar la imagen ISO, por ejemplo con `cd /tmp` y `mkdir iso`. También puede crear un subdirectorio para GRUB con `mkdir -p iso/boot/grub`. A continuación copie el archivo `stage2_eltorito` en el directorio `grub`:

```
cp /usr/lib/grub/stage2_eltorito iso/boot/grub
```

Copie también el kernel (`/boot/vmlinuz`), `initrd` (`/boot/initrd`) y el archivo `/boot/message` en el directorio `iso/boot/`:

```
cp /boot/vmlinuz iso/boot/
cp /boot/initrd iso/boot/
cp /boot/message iso/boot/
```

A fin de que GRUB pueda encontrar estos archivos, copie `menu.lst` en el directorio `iso/boot/grub` y modifique las rutas para que se puedan leer los archivos en el CD. Para ello sustituya en la ruta el nombre de dispositivo del disco duro (por ejemplo `(hd*)`) por el nombre de dispositivo de la unidad de CD-ROM `(cd)`:

```
gfxmenu (cd)/boot/message
timeout 8
default 0

title Linux
    kernel (cd)/boot/vmlinuz root=/dev/hda5 vga=794 resume=/dev/hda1
splash=verbose showopts
    initrd (cd)/boot/initrd
```

Finalmente, ejecute el siguiente comando para crear una imagen ISO:

```
mkisofs -R -b boot/grub/stage2_eltorito -no-emul-boot \
-boot-load-size 4 -boot-info-table -o grub.iso iso
```

Grabe el archivo resultante `grub.iso` en un CD con un programa de grabación cualquiera.

8.7. Pantalla de bienvenida de SUSE

Desde la versión 7.2 de SUSE LINUX, el sistema dispone de un arranque gráfico desde la primera consola si se emplea la opción "vga=<value>" como parámetro del kernel. Si está realizando la instalación mediante YaST, esta opción se activa automáticamente con la resolución y tarjeta gráfica elegidas. Existen tres formas de deshabilitar esta pantalla de bienvenida:

Desactivar la pantalla gráfica de SUSE cuando sea necesario
Introduzca el comando `echo 0 >/proc/splash` en la línea de comandos para desactivar el arranque gráfico. Para reactivarlo, emplee `echo 1 >/proc/splash`.

Desactivar la pantalla gráfica de SUSE de forma estándar
Añada el parámetro del kernel `splash=0` a la configuración del cargador de arranque. En el capítulo **??** en esta página puede encontrar más información al respecto. No obstante, si prefiere el modo texto (la opción predeterminada en versiones anteriores), establezca el valor de la variable como `vga=normal`.

Desactivar la pantalla gráfica de SUSE por completo
Compile un nuevo kernel y desactive la opción 'Use splash screen instead of boot logo' en 'framebuffer support'.

Sugerencia

Si deshabilita el soporte framebuffer en el kernel, el arranque gráfico quedará desactivado automáticamente. Recuerde que SUSE no puede prestarle asistencia técnica si su sistema emplea un kernel personalizado.

Sugerencia

8.8. Problemas posibles y sus soluciones

Este apartado incluye algunos de los problemas más comunes que pueden ocurrir al arrancar con GRUB así como una breve explicación de sus respectivas soluciones. Para algunos de estos problemas existe un artículo en la base de datos de soporte (`http://portal.suse.de/sdb/es/index.html`). Si tropieza con un problema que no aparece en la lista, le recomendamos buscar en la base de datos de soporte (`https://portal.suse.com/PM/page/search.pm`) con las palabras claves *GRUB*, *boot* o *bootloader*.

GRUB y XFS XFS no deja espacio para `stage1` en el bloque de arranque de la partición. Así pues, el cargador de arranque nunca ha de estar situado en una partición que contenga un sistema de archivos XFS. Una posible solución es crear una partición de arranque separada que no esté formateada con XFS (ver procedimiento en las líneas inferiores).

GRUB y JFS Aunque la combinación de GRUB con JFS es posible desde un punto de vista técnico, en la práctica resulta bastante problemática. En estos casos se recomienda crear una partición de arranque `/boot` separada, formateada con Ext2, e instalar GRUB en esta partición.

GRUB devuelve el mensaje GRUB Geom Error
GRUB sólo comprueba la geometría de los discos duros conectados en el momento del arranque. En algunos casos excepcionales, la BIOS devuelve entradas que no concuerdan por lo que GRUB informa sobre un GRUB Geom Error. Como solución, utilice LILO o actualice la BIOS si es necesario. Puede obtener información detallada sobre la instalación, configuración y mantenimiento de LILO introduciendo en la base de datos de soporte el término de búsqueda LILO.

GRUB también devuelve este mensaje de error cuando Linux ha sido instalado en un disco duro adicional que no está registrado en la BIOS. El sistema encuentra y carga la primera fase del cargador de arranque (*stage1*) correctamente pero no es capaz de hallar la segunda fase, *stage2*. En este caso, registre inmediatamente el nuevo disco duro en la BIOS.

Un sistema mixto IDE/SCSI no arranca
En ocasiones puede ocurrir que YaST detecte durante la instalación una secuencia de arranque equivocada de los discos duros (y que usted no la haya corregido). Así por ejemplo, para GRUB, `/dev/hda` será `hd0` y

`/dev/sda` será `hd1`, mientras que el orden en la BIOS es el opuesto (SCSI *antes* que IDE).

En este caso utilice la línea de comandos de GRUB para corregir los discos duros empleados durante el arranque y, una vez en el sistema arrancado, edite el archivo `device.map` para definir este orden de forma permanente. Por último, compruebe los nombres de dispositivo de GRUB en los archivos `/boot/grub/menu.lst` y `/boot/grub/device.map` y reinstale el cargador de arranque ejecutando el comando:

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

Arrancar Windows desde el segundo disco duro

Algunos sistemas operativos (como por ejemplo Windows) sólo pueden arrancar del primer disco duro. Si ha instalado uno de estos sistemas operativos en un disco duro distinto al primero, puede realizar un cambio lógico en la entrada de menú correspondiente.

```
...
title windows
   map (hd0) (hd1)
   map (hd1) (hd0)
   chainloader(hd1,0)+1
...
```

En este caso, Windows ha de arrancar del segundo disco duro, para lo que se cambia la secuencia de arranque lógica de los discos duros con `map`. No obstante, tenga en cuenta que este cambio *no* modifica la lógica del archivo de menú de GRUB. Así, en `chainloader` todavía debe constar el segundo disco duro.

8.9. Información adicional

La página web `http://www.gnu.org/software/grub/` contiene abundante información sobre GRUB en inglés. En caso de que texinfo esté instalado en el sistema, puede utilizar el comando `info grub` para ver en la shell las páginas de información sobre GRUB. También puede consultar nuestra base de datos de soporte `http://portal.suse.de/sdb/en/index.html` introduciendo el término de búsqueda *GRUB*.

El kernel de Linux

El kernel se encarga de administrar el hardware en los sistemas Linux y de ponerlo a disposición de los diversos procesos. Las siguientes páginas no le servirán para convertirse en un hacker del kernel, pero le ayudarán a realizar una actualización del mismo y a ser capaz de compilar e instalar un kernel configurado. Si sigue las instrucciones de este capítulo, el kernel funcionará adecuadamente y lo podrá arrancar en cualquier momento.

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.

A veces es posible modificar el comportamiento del kernel instalado por medio de parámetros del kernel. Por ejemplo, el parámetro `desktop` reduce los intervalos de tiempo del planificador, lo que redunda en una mayor velocidad subjetiva del sistema. Si el paquete `kernel-source` está instalado, puede obtener información adicional en la documentación del kernel en el directorio `/usr/src/linux/Documentation`.

Ya existen `makefiles` para la creación de un nuevo kernel; con ayuda de éstas 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.

9.1. Actualización del kernel

Para instalar un kernel actualizado de SUSE, utilice la característica de actualización en línea de YaST. Una vez realizada la actualización, tendrá que reiniciar el sistema, ya que el antiguo kernel aún se estará ejecutando y no será capaz de encontrar los módulos apropiados para el proceso. Si desea obtener más información acerca de la función de actualización en línea de YaST, consulte la sección 2.2.3 en la página 49.

Cuando se ejecute la actualización, se mostrará una ventana emergente que describe todas las acciones que es necesario llevar a cabo. Es importante que las siga a fin de mantener la consistencia del sistema.

9.2. 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 como el compilador de C (`gcc`), los GNU Binutils (`binutils`) y las librerías de C (Include-files) (`glibc-devel`), se instalarán automáticamente.

Tras la instalación, las fuentes del kernel se encuentran en el directorio `/usr/src/linux-<versión_kernel>`. 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.

9.3. Configuración del kernel

La configuración del kernel ejecutándose actualmente se encuentra en el archivo `/proc/config.gz`. Para modificar esta configuración conforme a sus necesidades, cambie como usuario `root` al directorio `/usr/src/linux` y ejecute el siguiente comando:

```
zcat /proc/config.gz > .config
make oldconfig
```

El comando `make oldconfig` utiliza el archivo `/usr/src/linux/.config` como plantilla para la configuración actual del kernel. En caso de haber añadido nuevas opciones a las fuentes del kernel empleadas actualmente, el script le pregunta ahora sobre las mismas.

Dada su extensión, este capítulo no se ocupa en detalle de la configuración de las opciones del kernel. Le recomendamos que consulte la abundante documentación que existe acerca de este tema. Puede encontrar la última versión de ésta en `/usr/src/linux/Documentation`.

9.3.1. Configuración en la línea de comandos

Para configurar el kernel, cambie a `/usr/src/linux` e introduzca el 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) (yes), (n) (no) o (m) (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.

9.3.2. 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.

9.3.3. Configuración en el sistema X Window

Si en su sistema están instalados y configurados el sistema X Window (paquete `xorg-x11`) y los paquetes de desarrollo de QT (`qt3-devel`), también puede iniciar el proceso de instalación con el comando `make xconfig`. De este modo dispone de una interfaz gráfica más cómoda desde el punto de vista de la configuración pero es preciso iniciar el sistema X Window como superusuario `root` o bien introducir primero en Shell `su` para poder tener acceso a la pantalla como `root`-shell. 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 de la configuración realizada con `make xconfig` no es tan bueno como con las otras opciones de configuración. Por este motivo, siempre debería ejecutar un `make oldconfig` después de este método de configuración.

9.4. 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. El controlador de los discos duros, soporte para `ext2`, los controladores SCSI en un sistema SCSI y similares se suelen compilar directamente en el kernel; mientras que el soporte para `isofs`, `msdos` o `sound` se debe compilar como módulo.

Sugerencia

Incluso los controladores que son necesarios para arrancar el sistema pueden ser incluidos en el kernel como módulos. En este caso, el ramdisk inicial se emplea para cargarlos durante el arranque.

Sugerencia

Los módulos del kernel se guardan en el directorio `/lib/modules/<versión>`, donde `versión` corresponde a la versión actual del kernel.

9.4.1. 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 comando `hwinfo --scsi`. La salida de este programa de ayuda se encuentra también en el módulo de información de hardware de YaST.

9.4.2. Manejo de los módulos

El paquete `module-init-tools` incluye las utilidades necesarias para cargar módulos en el kernel. 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//<versión>`. Se recomienda dejar de usar `insmod` en favor del comando `modprobe` ya que éste comprueba también las dependencias del módulo.

rmmod Este comando descarga el módulo indicado, lo cual sólo es posible cuando se ha dejado de usar esta función del módulo, y no es posible descargar por ejemplo 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 (por ejemplo para probar todos los módulos de un determinado tipo hasta que se cargue uno exitosamente). Al contrario de insmod, modprobe evalúa el archivo `/etc/modprobe.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 daemon del kernel 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.

modinfo Muestra información sobre un módulo. Puesto que la información mostrada se extrae del mismo módulo, sólo es posible mostrar información que haya sido integrada por los desarrolladores del controlador. Entre los datos que pueden estar presentes se incluyen el autor, una descripción, la licencia, parámetros del módulo, dependencias y alias.

9.4.3. /etc/modprobe.conf

Los archivos `/etc/modprobe.conf`, `/etc/modprobe.conf.local` y el directorio `/etc/modprobe.d` controlan la carga de módulos (ver la página del

manual `man modprobe.conf`). Este archivo permite indicar los parámetros para aquellos módulos que acceden directamente al hardware y por lo tanto deben ser adaptados específicamente al ordenador (por ejemplo 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`.

9.4.4. Kmod – el cargador de módulos del kernel (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.

9.5. Compilación del kernel

► **x86, AMD64, EM64T**
Se recomienda la compilación de una imagen "bzImage". Normalmente, esto evita el problema de que el tamaño del kernel resulte demasiado grande. Esta circunstancia puede producirse si se seleccionan demasiadas características y se crea una imagen "zImage". Si este hecho llegara a producirse, se mostrarían mensajes acerca de un tamaño excesivo de kernel o sistema. ◄

Una vez personalizado el kernel tal y como se describe en la sección **??** en esta página, debe iniciar la compilación en `/usr/src/linux/`:

```
make clean
make bzImage
```

Puede introducir también ambos comandos en una sola línea:

```
make clean bzImage
```

Después de una compilación correcta, puede encontrar el kernel comprimido en `/usr/src/linux/arch/<arch>/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 trabaja con el bash, puede utilizar:

```
make bzImage V=1 2>&1 | tee kernel.out
```

para volver a iniciar el proceso de compilación y dejar que se escriba en el archivo `kernel.out`.

Si hay funciones del kernel que se realizan con módulos, es preciso compilarlos, lo cual se consigue con el comando `make modules`.

9.6. Instalación del kernel

A continuación debe instalarse el kernel en el directorio `/boot`. Para ello ejecute el comando:

```
INSTALL_PATH=/boot make install
```

Los módulos compilados también se deben instalar. El comando `make modules_install` los copia en los directorios de destino correctos (`/lib/modules//<version>`). 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.

Sugerencia

Si se incorporan módulos al kernel, es necesario eliminarlos de `/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.

Sugerencia

A fin de que GRUB pueda arrancar el antiguo kernel (actualmente `/boot/vmlinuz.old`), introduzca en el archivo `/boot/grub/menu.lst` una etiqueta

adicional `Linux.old` como imagen de arranque. Este proceso se describe detalladamente en el capítulo **??** en esta página. En este caso no es necesario volver a instalar GRUB.

Asimismo, debe tenerse en cuenta lo siguiente: el archivo `/boot/System.map` contiene los símbolos requeridos por los módulos del kernel para poder activar correctamente las funciones del kernel. Este archivo depende del kernel actual. Por este motivo, una vez compilado e instalado el kernel, es necesario copiar el actual archivo `/usr/src/linux/System.map` en el directorio `/boot`. Cada vez que el kernel se compile, este archivo se creará de nuevo. Si al arrancar obtiene un mensaje de error del estilo a "System.map does not match actual kernel", probablemente el archivo `System.map` no haya sido copiado a `/boot` después de compilar el kernel.

9.7. 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 mediante el comando `make clean` en el directorio `/usr/src/linux`. 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.

Particularidades de SUSE LINUX

Este capítulo le proporciona información sobre algunos paquetes de software así como sobre las consolas virtuales y la disposición del teclado. Al final del capítulo encontrará además una sección relativa a las opciones de personalización en función del idioma y el país (I18N y L10N).

10.1. Información sobre paquetes especiales

10.1.1. El paquete bash y /etc/profile

La siguiente lista muestra todos los archivos init que bash evalúa cuando se usa como shell de login. Bash procesa estos archivos en el orden indicado en la lista.

1. `/etc/profile`
2. `~/.profile`
3. `/etc/bash.bashrc`
4. `~/.bashrc`

Los usuarios pueden efectuar sus propias entradas en `~/.profile` o en `~/.bashrc`. Para garantizar que estos archivos sean procesados correctamente, recomendamos reproducir la configuración básica de `/etc/skel/.profile` o `/etc/skel/.bashrc` en el directorio del usuario. Por tanto, después de una actualización le aconsejamos adoptar las opciones de configuración de `/etc/skel`. Para no perder las opciones personalizadas, 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 esto, puede copiar las opciones personalizadas de los archivos `*.old`.

10.1.2. El paquete cron

Las tablas de `cron` se encuentran en `/var/cron/tabs`. El archivo `/etc/crontab` se configura como tabla válida para todo el sistema. En este archivo hay que introducir, además de la hora, como qué usuario ha de ejecutarse la tarea correspondiente (ver ejemplo **??** en esta página, en el que figura `root` como usuario). Las tablas específicas de los paquetes (en `/etc/cron.d`) tienen el mismo formato. Ver la página del manual `man cron`.

Ejemplo 10.1: *Ejemplo de entrada en /etc/crontab*

```
1-59/5 * * * * root test -x /usr/sbin/atrun && /usr/sbin/atrun
```

No se puede usar el comando `crontab -e` para modificar `/etc/crontab`. Se debe modificar y guardar con un editor.

Algunos paquetes 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/contrab`). Esto garantiza que los procesos que hayan podido desatenderse se ejecuten en el momento adecuado.

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, por ejemplo los componentes `backup-rpmdb`, `clean-tmp` o `clean-vi`.

10.1.3. Archivos de registro: el paquete logrotate

Muchos servicios del sistema (daemons) y el mismo kernel vuelcan periódicamente el estado del sistema y sucesos especiales en archivos de registro (logfiles). Así el administrador puede controlar de forma eficaz el estado del 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 de tamaño. Con ayuda del `logrotate` se puede controlar el crecimiento de los archivos de registro.

Configuración

El archivo de configuración `/etc/logrotate.conf` define el comportamiento general. Mediante la indicación `include` se determina principalmente qué archivos se deben evaluar; en SUSE LINUX está previsto que los paquetes individuales instalen archivos en `/etc/logrotate.d` (por ejemplo `syslog` o `yast`).

Ejemplo 10.2: *Ejemplo de /etc/logrotate.conf*

```
# see "man logrotate" for details
# rotate log files weekly weekly
# keep 4 weeks worth of backlogs rotate 4
# create new (empty) log files after rotating old ones create
# uncomment this if you want your log files compressed
#compress
# RPM packages drop log rotation information into this directory
include /etc/logrotate.d
# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#    monthly
#    create 0664 root utmp
#    rotate 1
#}
# system-specific logs may be also be configured here.
```

logrotate se controla con cron; se arranca una vez al día mediante `/etc/cron.daily/logrotate`.

Importante

La opción `create` carga de los archivos `/etc/permissions*` posibles opciones de configuración efectuadas como administrador. Asegúrese de que no se produzcan conflictos al realizar sus propios ajustes.

Importante

10.1.4. Páginas man

Para algunos programas GNU no se siguen manteniendo las páginas man (por ejemplo tar). En su lugar se puede usar como ayuda rápida la extensión `--help` o los archivos de tipo info. Info (`info`) es el sistema de hipertexto de GNU cuyo uso se explica con el comando `info info`. Las páginas info se pueden ver en Emacs con el comando `emacs -f info` o bien introduciendo `info`. También puede utilizar tkinfo, xinfo o el acceso a través del sistema de ayuda de SUSE para ver páginas info.

10.1.5. El comando locate

El comando locate para encontrar archivos rápidamente no está incluido en la instalación estándar. Instálelo en caso necesario (`find-locate`). Al hacerlo, se iniciará un proceso updatedb todas las noches o bien 15 minutos después de encender el ordenador.

10.1.6. El comando ulimit

El comando `ulimit` (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 puede ejecutarse con varias opciones. Por ejemplo, las que limitan el gasto de memoria figuran en la tabla **??** en esta página.

Cuadro 10.1: *ulimit: Limitar los recursos para el usuario*

`-m`	Tamaño máximo de memoria RAM
`-v`	Tamaño máximo de la memoria virtual
`-s`	Tamaño máximo de la pila
`-c`	Tamaño máximo de los archivo core
`-a`	Mostrar límites establecidos

Los límites para todo el sistema se pueden definir en `/etc/profile`. También es en este archivo donde se debe dar de alta la creación de los archivos core que necesitan los programadores para depurar (debug) código. Los usuarios no pueden aumentar los valores que el administrador del sistema define en `/etc/profile`, pero sí que pueden insertar entradas especiales en su propio `~/.bashrc`.

Ejemplo 10.3: *Opciones de configuración de ulimit en ~/.bashrc*

```
# Limitar la memoria RAM
ulimit -m 98304

# Limitar la memoria virtual
ulimit -v 98304
```

Todos los valores se han de indicar en KB. Puede obtener información más detallada la página del manual `man bash`.

Importante

No todas las shells soportan instrucciones `ulimit`. Si debe realizar una configuración más compleja, PAM (por ejemplo `pam_limits`) le ofrece más posibilidades.

Importante

10.1.7. El comando free

El comando `free` es bastante equívoco cuando se trata de averiguar cómo se está utilizando la memoria RAM. Puede encontrar información útil en `/proc/meminfo`. Hoy en día no se debería preocupar por esto ningún usuario que utilice un sistema operativo moderno como Linux. El concepto de memoria de trabajo libre viene de la época en que aún no existía ningún administrador de memoria unificado (unified memory management). En Linux existe el lema: *memoria libre es memoria mala* (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 escasea, algunas partes se escriben en la zona de intercambio (swap) o en los archivos de los cuales leía al principio con ayuda de `mmap` (ver `man mmap`).

Además el kernel dispone de otra memoria caché adicional, como la "slab cache", que por ejemplo 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 consultar en `/proc/slabinfo`.

10.1.8. El archivo /etc/resolv.conf

La resolución de nombres se regula en el archivo `/etc/resolv.conf`; véase apartado capítulo **??** en esta página. Sólo el script `/sbin/modify_resolvconf` se encarga de modificar el archivo `/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 coherentes si se cumple siempre esta regla.

10.1.9. Configuración de GNU Emacs

GNU Emacs es un entorno de trabajo bastante complejo. Puede encontrar más información sobre el mismo en: `http://www.gnu.org/software/emacs/`. En los siguientes párrafos se explican los archivos de configuración que GNU Emacs procesa durante el inicio.

Al iniciarse, Emacs lee diversos archivos con la configuración del usuario, administrador de sistemas o del distribuidor a efectos de personalización o preconfiguración. El archivo de inicio `~/.emacs` se instala en el directorio local de cada usuario desde `/etc/skel`; `.emacs` lee a su vez el archivo `/etc/skel/.gnu-emacs`. Si un usuario desea modificar este archivo, se recomienda copiarlo en el propio directorio local de usuario (con `cp /etc/skel/.gnu-emacs ~/.gnu-emacs`) y realizar allí los cambios deseados.

El archivo `~/.gnu-emacs-custom` se crea en `.gnu-emacs` como `custom-file`. Si el usuario quiere realizar su propia configuración por medio de las opciones `customize`, los cambios se guardarán en `~/.gnu-emacs-custom`.

Junto con el paquete `emacs` se instala en SUSE LINUX el archivo `site-start.el` en el directorio `/usr/share/emacs/site-lisp`. El archivo `site-start.el` se carga antes que el archivo de inicio `~/.emacs`. `site-start.el` se ocupa, por ejemplo, de cargar automáticamente archivos de configuración que han sido instalados con paquetes complementarios de Emacs incluidos en la distribución como `psgml`. Tales archivos 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`.

Puede obtener información adicional sobre estos archivos en el archivo info de Emacs en el nodo *Init File*: `info:/emacs/InitFile`. 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.
- `emacs-info`: documentación en línea en formato info.
- `emacs-el` contiene los archivos de librerías no compiladas en Emacs Lisp. Actualmente no es necesario.
- Numerosos paquetes adicionales que pueden ser instalados en caso necesario: `emacs-auctex` (para LaTeX); `psgml` (para SGML/XML); `gnuserv` (para el uso de cliente y servidor), etc.

10.1.10. Introducción a vi

Los editores de texto se emplean todavía para realizar numerosas tareas de administración de sistemas así como para programar. En los entornos Unix, vi se cristalizó como un editor estándar que, además de ofrecer cómodas funciones de edición, resulta incluso más ergonómico que algunos editores que se controlan con el ratón.

Modos de operación

vi distingue tres modos de uso diferentes: el modo de *inserción* (insert), el modo de *comandos* (command)y el modo *extendido* (extended). Las teclas tienen significados diferentes dependiendo del modo de operación. Después de arrancarlo, vi se encuentra normalmente en el modo *command*. Lo primero que debe aprenderse es a pasar de un modo a otro:

Modo command a modo insert Para cambiar del modo *command* a *insert* existen múltiples posibilidades: puede pulsar por ejemplo (A) (append) para añadir, (I) para insertar o bien (O) para insertar una línea nueva por debajo de la línea actual.

Modo insert a modo command Para salir del modo *insert* pulse la tecla (Esc). No es posible salir de vi en modo *insert*, por eso es importante acordarse siempre de pulsar (Esc) antes de cualquier operación.

Modo command a modo extended Puede acceder al modo *extendido* de vi introduciendo un signo de dos puntos ((:)). Este modo, también llamado *ex*, es como un editor de línea de comandos independiente que puede utilizarse para tareas de diversa complejidad.

Modo extended a modo command Después de haber ejecutado un comando en modo *extended*, el usuario vuelve al modo *command*. Si accede al modo extendido por error, borre los dos puntos con la tecla de retroceso (←) para volver así al modo de comandos.

El cambio del modo *insert* al modo *extended* siempre requiere pasar por el modo *command*. Un cambio directo no está previsto.

Al igual que otros editores, vi tiene su propio mecanismo para terminar el programa. Así, no es posible salir de vi en el modo *insert* sino que es necesario salir primero del modo *insert* con la tecla Esc. A continuación dispone de dos opciones:

1. *Salir sin guardar:* para salir del editor sin guardar los cambios, introduzca en el modo *command* : W Q. En el modo *extended*, W significa "write" y Q "quit" (salir).
2. *Guardar y salir:* existen varias posibilidades para guardar los cambios y salir del editor. En el modo *command*, utilice Shift Z Z. Para salir del programa y guardar los cambios desde el modo *extended*, introduzca : W Q. En el modo *extended*, W significa "write" (escribir) y Q "quit" (salir).

vi en acción

vi puede utilizarse como un editor normal. Una vez que se encuentre en modo *insert* puede introducir texto y borrarlo con las teclas ← y Supr. El cursor se mueve con las teclas de control del cursor (flechas).

En ocasiones, precisamente estas teclas son una posible fuente de problemas. Esto se debe a la multitud de tipos de terminal y a sus códigos de teclas especiales. Este problema puede evitarse con el modo *command*. Pulse Esc para pasar del modo *insert* al modo *command*. En este modo se puede mover el cursor con las teclas H, J, K y L con el siguiente significado:

H un carácter hacia la izquierda

J una línea hacia abajo

K una línea hacia arriba

L un carácter hacia la derecha

Los comandos del modo *command* de vi pueden tener ciertas variaciones. Por ejemplo, para ejecutar un comando varias veces se puede introducir el número de repeticiones como cifra y después el propio comando. La secuencia de comandos 5L hace que el cursor se mueva cinco caracteres a la derecha.

Información adicional

vi soporta una amplia variedad de comandos. Permite el uso de macros, atajos de teclado, búferes y un sinfín de características cuya descripción sería demasiado larga para este capítulo. SUSE LINUX utiliza una versión mejorada de vi llamada vim (vi improved). Existen numerosas fuentes de información sobre este editor:

- vimtutor es un programa de aprendizaje interactivo para vim.
- El comando `:help` de vim muestra una ayuda extensa sobre muchos temas.
- En la URL `http://www.truth.sk/vim/vimbook-OPL.pdf` se encuentra un libro (en inglés) sobre vim.
- La página web del proyecto vim, `http://www.vim.org`, muestra todas las novedades e incluye listas de correo y documentación adicional.
- En Internet se encuentran algunos tutoriales sobre vim. Entre ellos cabe destacar: `http://www.selflinux.org/selflinux/html/vim.html`, `http://www.linuxgazette.com/node/view/9039` y `http://www.apmaths.uwo.ca/~xli/vim/vim_tutorial.html`. Una lista de enlaces adicionales está disponible en `http://linux-universe.com/HOWTO/Vim-HOWTO/vim-tutorial.html`.

Importante

La licencia de VIM

vim representa un tipo de software llamado "Charityware". Esto significa que los autores no quieren recibir dinero por su trabajo sino que le animan a realizar un donativo para un proyecto humanitario. En este caso se trata de un proyecto de apoyo a niños en Uganda. Puede encontrar información sobre este proyecto en Internet en `http://iccf-holland.org/index.html`, `http://www.vim.org/iccf/` y `http://www.iccf.nl/`.

Importante

10.2. Consolas virtuales

Linux es un sistema multitarea y multiusuario. Las ventajas que aportan estas prestaciones se agradecen incluso en ordenadores 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 archivo `/etc/inittab` se puede disponer de más o menos consolas. Si estando en X11 desea trabajar en una consola virtual sin cerrar X11, pulse las combinaciones (Ctrl)-(Alt)-(F1) a (Ctrl)-(Alt)-(F6). Para volver a X11, pulse (Alt)-(F7).

10.3. Distribución del teclado

Para normalizar la distribución del teclado de los distintos programas, se han modificado, entre otros, los siguientes archivos:

```
/etc/inputrc
/usr/X11R6/lib/X11/Xmodmap
/etc/skel/.Xmodmap
/etc/skel/.exrc
/etc/skel/.less
/etc/skel/.lesskey
/etc/csh.cshrc
/etc/termcap
/usr/lib/terminfo/x/xterm
/usr/X11R6/lib/X11/app-defaults/XTerm
/usr/share/emacs/<VERSION>/site-lisp/term/*.el
```

Estas modificaciones sólo tienen efecto sobre las aplicaciones que utilizan las entradas `terminfo` o sobre aquellas cuyos archivos de configuración se modifican directamente (`vi`, `less`, etc.). Se recomienda adaptar otras aplicaciones no incluidas en SUSE LINUX a estas definiciones.

Dentro del entorno X se puede acceder a la tecla compose (multikey) mediante la combinación de teclas (Ctrl)-(Shift) (derecha). Véase a este respecto la entrada correspondiente en `/usr/X11R6/lib/X11/Xmodmap`.

"X Keyboard Extension" (XKB) permite acceder a opciones de configuración avanzadas. Esta extensión es también utilizada por los escritorios GNOME (gswitchit) y KDE (kxkb). Puede obtener información adicional sobre XKB en el archivo `/etc/X11/xkb/README` así como en los documentos allí mencionados.

Puede encontrar información sobre la introducción de los idiomas chino, japonés o coreano (CJK) en la página web de Mike Fabian: `http://www.suse.de/~mfabian/suse-cjk/input.html`.

10.4. Configuración en función del idioma y el país

SUSE LINUX presenta un alto nivel de internacionalización y puede adaptarse a las necesidades locales de forma muy flexible. En otras palabras, la internacionalización (I18N) permite implementar extensiones locales (L10N). Las abreviaturas I18N y L10N sustituyen a los términos *internationalization* y *localization* y están formadas por la letra inicial y final de cada término así como por el número de caracteres entre ambas.

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 (native language support), 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 archivo `language` mediante una variable individual o de forma indirecta mediante una variable de un nivel más alto (véase la página del manual `man locale`).

`RC_LC_MESSAGES`, `RC_LC_CTYPE`, `RC_LC_COLLATE`, `RC_LC_TIME`, `RC_LC_NUMERIC`, `RC_LC_MONETARY`
: Estas variables se pasan a la shell sin el prefijo `RC_` y determinan las categorías arriba mencionadas. A continuación se detalla el significado de las distintas variables.

`RC_LANG` En caso de estar definida, esta variable sobreescribe los valores de las variables mencionadas arriba.

`RC_LANG` Si no se define ninguna de las variables arriba mencionadas, esta sirve de definición de reserva (fallback). SUSE LINUX sólo define por defecto `RC_LANG`. De esta forma es más fácil para el usuario introducir valores propios.

`ROOT_USES_LANG` Una variable booleana de valor `yes` o `no`. Si tiene el valor `no`, `root` siempre trabaja en el entorno POSIX.

Las demás variables se determinan mediante el editor `sysconfig` de YaST. El valor de estas variables contiene la identificación del idioma (language code), la

del país o territorio (country code), el conjunto de caracteres (encoding) y la opción (modifier). Todas estas indicaciones se unen mediante caracteres especiales:

```
LANG=<language>[[_<COUNTRY>].<Encoding>[@<Modifier>]]
```

10.4.1. 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`). Sólo se puede seleccionar valores que encuentran su homólogo en un archivo de descripción dentro del directorio `/var/lib/locale`. Es posible crear archivos de descripción a partir de los archivos `/usr/share/i18n` usando `localedef`; los archivos de descripción forman parte del paquete `glibc-i18ndata`. Por ejemplo, un archivo de descripción para `es_ES@euro.UTF-8` se crea mediante el comando:

```
localedef -i es_ES@euro -f UTF-8 es_ES@euro.UTF-8
```

`LANG=es_ES.UTF-8` Esta es la opción predeterminada cuando se instala en castellano. Si la instalación se realiza en otro idioma, UTF-8 sigue siendo el juego de caracteres seleccionado y el otro idioma se adopta para el sistema.

`LANG=es_ES.ISO-8859-1` De este modo se configura el idioma español para España con el juego de caracteres `ISO-8859-1`. Este aún no incorpora el símbolo del Euro pero sigue siendo necesario para los programas que aún no han sido adaptados a `UTF-8`. Por ejemplo, el programa Emacs es uno de los que lee la opción de configuración del juego de caracteres (aquí `ISO-8859-1`).

`LANG=es_ES@euro` El ejemplo superior incluye explícitamente el signo del euro en un juego de caracteres. En sentido estricto, esta opción resulta obsoleta ya que UTF-8 comprende también el signo del euro. No obstante, puede serle de utilidad si una aplicación no soporta UTF-8 sino, por ejemplo, ISO-8859-15.

SuSEconfig lee las variables de `/etc/sysconfig/language` y escribe los valores en los archivos `/etc/SuSEconfig/profile` y `/etc/SuSEconfig/csh.`

cshrc. /etc/profile lee el archivo /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 archivo 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

10.4.2. Configuración del soporte de idioma

Los archivos de la categoría *mensajes* normalmente sólo se encuentran dentro del directorio de idioma (por ejemplo en) para tener una solución de reserva. Por ejemplo cuando el valor de LANG sea en_US y el archivo de mensajes en /usr/share/locale/en_US/LC_MESSAGES no exista, se recurrirá al archivo /usr/share/locale/en/LC_MESSAGES para los mensajes.

Una cadena de soluciones de reserva puede definirse, por ejemplo, para bretón → francés o para gallego → español → portugués:

```
LANGUAGE="br_FR:fr_FR"
```

```
LANGUAGE="gl_ES:es_ES:pt_PT"
```

O para – dependiendo de las preferencias – cambiar a las variantes noruegas nyorsk o bien bokmål (con no como alternativa):

```
LANG="nn_NO"
```

```
LANGUAGE="nn_NO:nb_NO:no"
```

o bien

```
LANG="nb_NO"
```

```
LANGUAGE="nb_NO:nn_NO:no"
```

En el caso del noruego también hay que tener en cuenta que LC_TIME se trata de forma diferente.

Posibles problemas

- En cadenas de números no se reconoce el punto como separador de miles. Probablemente el valor de LANG sea es. Como la descripción que usa la glibc se encuentra en /usr/share/lib/es_ES/LC_NUMERIC, LC_NUMERIC debe tener por ejemplo el valor es_ES.

Información adicional

- *The GNU C Library Reference Manual*, capítulo Locales and Internationalization, está incluido en `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 sistema X Window

El sistema X Window (X11) es prácticamente el estándar para interfaces gráficas de usuario en Unix. X es además un sistema basado en redes. Así, las aplicaciones que estén funcionando en un ordenador pueden mostrar sus datos de salida en otro siempre que ambas máquinas estén conectadas a través de una red. El tipo de red (LAN o Internet) es irrelevante.

En este capítulo se describe la configuración y algunas posibilidades de optimización para el sistema X Window junto con información sobre los tipos de letra en SUSE LINUX y la configuración 3D de OpenGL.

11.1. Configuración de X11 con SaX2

La interfaz gráfica de usuario o servidor X se ocupa de la comunicación entre el hardware y el software. Los escritorios como KDE y GNOME y la amplia variedad de gestores de ventanas se sirven del servidor X para interactuar con el usuario.

La interfaz gráfica se configura ya durante la instalación. SaX2 le permite modificar la configuración posteriormente. Los valores de configuración actuales están guardados y puede restaurarlos en cualquier momento. Los valores mostrados para su modificación son los siguientes: resolución de pantalla, profundidad de color, frecuencia de repetición y fabricante y modelo del monitor, en caso de que haya sido detectado automáticamente.

Si acaba de instalar una nueva tarjeta gráfica, aparecerá una pequeña ventana preguntándole si desea activar la aceleración 3D para la misma. Tras pulsar en 'Cambiar', SaX2, la herramienta de configuración para los dispositivos gráficos y de entrada, se inicia en una ventana separada que se muestra en la figura **??** en esta página.

La barra de navegación de la izquierda contiene cuatro elementos: 'Escritorio', 'Dispositivos de entrada', 'Multimonitor' y 'Control de acceso'. En 'Escritorio' puede configurar el monitor, la tarjeta gráfica, la profundidad de color y la resolución, el tamaño de la imagen, etc. En 'Dispositivos de entrada' puede configurar el teclado y el ratón así como un monitor de pantalla táctil (touchscreen) y una tableta gráfica. En el menú 'Multimonitor' puede configurar una estación multimonitor (ver sección **??** en esta página). El programa AccessX del 'Control de acceso' es una útil herramienta para controlar el puntero del ratón con el bloque de teclas numéricas.

Seleccione el modelo apropiado para el monitor y la tarjeta gráfica. Por lo general, el sistema los detectará automáticamente. En caso de que el sistema no detecte el monitor, aparecerá el diálogo de selección de monitores con una larga lista de fabricantes y modelos en la que muy probablemente encontrará el suyo. Si no es así, introduzca manualmente los valores correspondientes al monitor o escoja la configuración estándar denominada modo VESA.

Una vez completada la configuración del monitor y de la tarjeta gráfica en la ventana principal, pulse 'Finalizar' para probar la configuración. De este modo, puede comprobar que la configuración escogida funciona sin problemas con el hardware. Si la imagen que aparece no es estable, interrumpa la prueba con la tecla Esc y reduzca el valor de la frecuencia de repetición de la imagen o la resolución o profundidad de color. Todos los cambios realizados – se haya hecho la prueba

Figura 11.1: *La ventana principal de SaX2*

o no – se activarán cuando reinicie el sistema gráfico o servidor X. Si utiliza KDE, basta con finalizar la sesión en iniciar una nueva.

11.1.1. Escritorio

Seleccionando 'Cambiar configuración' → 'Propiedades', aparece una ventana con tres lengüetas: 'Modelo de monitor', 'Frecuencias' y 'Experto':

'Modelo de monitor' Escoja el fabricante en la parte izquierda de la ventana, y el modelo en la parte derecha. En caso de que tenga un disquete con controladores de Linux para el monitor, utilícelo pulsando en 'Disco del fabricante'.

'Frecuencias' Introduzca aquí las frecuencias horizontales y verticales adecuadas para el monitor. La frecuencia vertical se corresponde con la frecuencia de repetición de la imagen. Normalmente estos valores vienen determinados por el modelo de monitor, por lo que no necesitará cambiar nada.

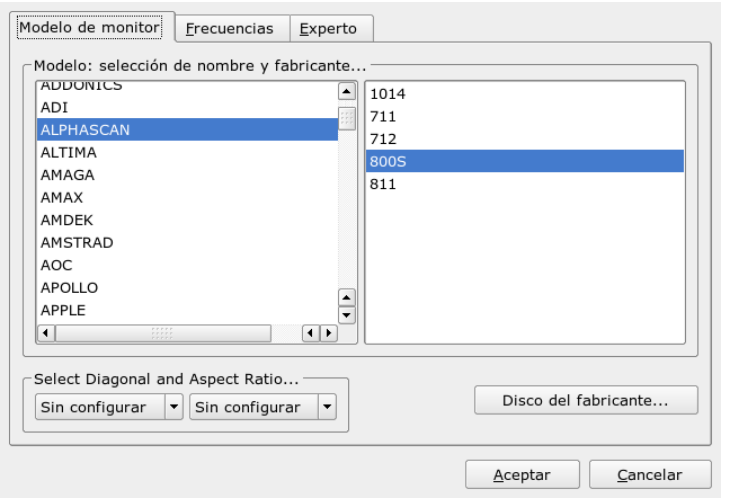

Figura 11.2: *SaX2: selección del monitor*

'Experto' Aquí aún puede configurar más opciones para el monitor. En el campo de selección que se encuentra en la parte superior puede establecer el método de cálculo de la resolución y de la geometría de la pantalla que se debe utilizar. Realice aquí modificaciones sólo si el monitor presenta problemas. Más abajo puede cambiar el tamaño de la imagen y activar el modo de ahorro de energía DPMS.

Aviso

Configuración de las frecuencias del monitor

A pesar de los mecanismos de protección integrados, debe actuar con especial precaución a la hora de configurar manualmente las frecuencias del monitor. Si se introducen valores erróneos, podría causar daños irreparables en el mismo. Si es necesario, consulte el manual del monitor antes de introducir los valores de las frecuencias.

Aviso

11.1.2. Tarjeta gráfica

En el diálogo de la tarjeta gráfica aparecen dos lengüetas: 'General' y 'Experto'. En 'General' puede seleccionar a la izquierda el fabricante y a la derecha el modelo de la tarjeta gráfica.

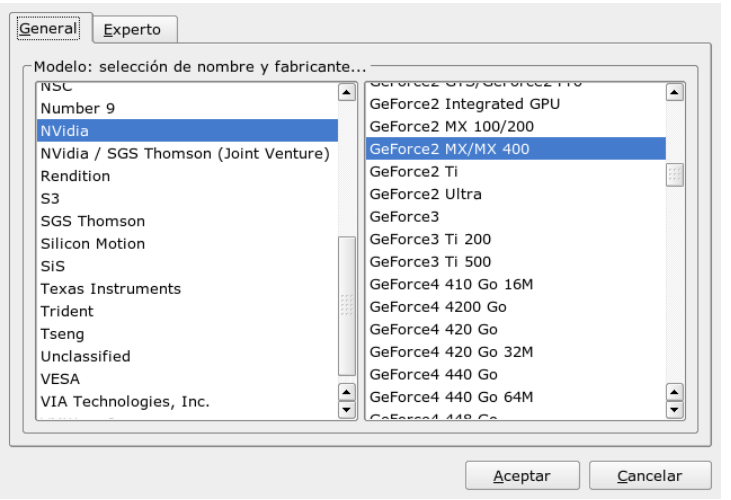

Figura 11.3: *SaX2: selección de la tarjeta gráfica*

La opción 'Experto' le ofrece posibilidades de configuración avanzada. A la derecha puede configurar si desea girar la pantalla hacia la izquierda o perpendicularmente (una opción útil para algunas pantallas TFT giratorias). Las entradas para el BusID sólo tienen relevancia si trabaja con más de una pantalla. Por lo general no necesita cambiar nada en este apartado. En particular le recomendamos no modificar nada si no conoce el significado de las distintas opciones. Si es necesario, lea en la documentación de su tarjeta gráfica qué significan las distintas opciones.

11.1.3. Color y resolución

Hay tres lengüetas disponibles: 'Color', 'Resoluciones...' y 'Experto'.

'Color' En función del hardware utilizado, dispone de las siguientes opciones para la profundidad de color: 16, 256, 32768, 65536 y 16,7 millones de colores a 4, 8, 15, 16 ó 24 bits. Debe elegir al menos 256 colores.

'Resoluciones...' Puede elegir entre todas las combinaciones de resolución y profundidad de color que el hardware puede mostrar sin problemas. De ahí que en SUSE LINUX se reduzca al mínimo el riesgo de dañar el hardware debido a una configuración inadecuada. Si aún así prefiere cambiar la resolución manualmente, infórmese en la documentación del hardware de los valores que puede utilizar.

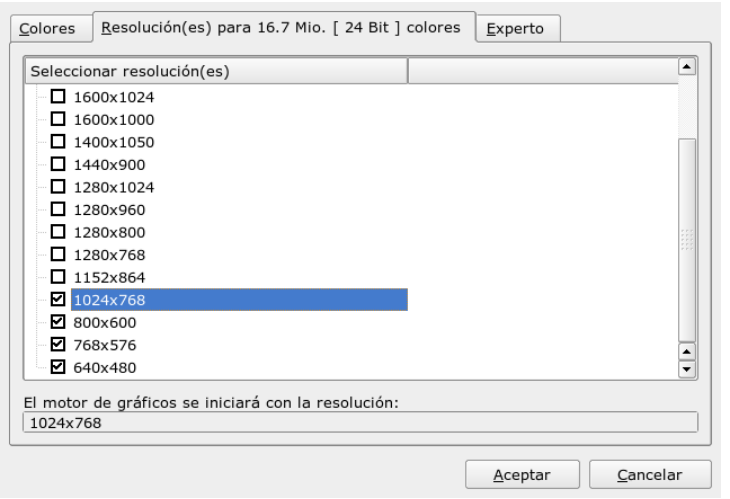

Figura 11.4: *SaX2: configuración de la resolución*

'Experto' Aquí puede añadir resoluciones a las ofrecidas en la lengüeta anterior para que se muestren en la lista de selección.

11.1.4. Resolución virtual

Todos los escritorios poseen una resolución propia visible en toda la pantalla. Junto a esta resolución se puede configurar otra resolución que sea mayor que el área visible de la pantalla. Si sale con el cursor de la pantalla, se moverá el área

virtual a la zona visible. De esta forma se incrementa el espacio de trabajo disponible.

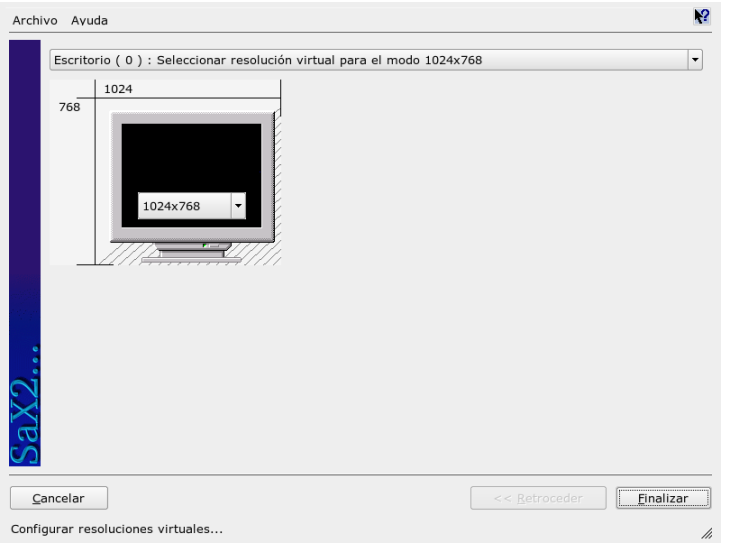

Figura 11.5: *SaX2: configuración de la resolución virtual*

La configuración de la resolución virtual se puede realizar de dos formas. El primer método, 'mediante drag&drop', consiste en situar el ratón sobre la imagen del monitor para que el puntero del ratón se transforme en un retículo. A continuación pulse el botón izquierdo del ratón al tiempo que mueve el ratón para modificar el tamaño de la superficie marcada. Esta superficie muestra el área de resolución virtual. Este método es el más adecuado si no está seguro de cuánto espacio virtual desea en el escritorio.

'Mediante selección en el menú desplegable': con el menú desplegable en el centro de la superficie marcada podrá ver la resolución virtual configurada actualmente. Si ya conoce la resolución estándar que quiere definir como resolución virtual, selecciónela en el menú.

11.1.5. Aceleración 3D

Si en la primera instalación o al acoplar la tarjeta gráfica con su correspondiente configuración no ha activado la aceleración 3D, puede hacerlo aquí.

11.1.6. Geometría

Aquí puede ajustar en las dos lengüetas (‘Cambiar posición’ y ‘Cambiar tamaño’) el tamaño y la posición de la imagen con ayuda de las flechas (ver figura **??** en esta página). Si trabaja con un entorno multimonitor, puede pasar a los monitores siguientes con el botón ‘Próxima pantalla’ para definir su tamaño y posición. Pulse ‘Grabar’ para guardar la configuración realizada.

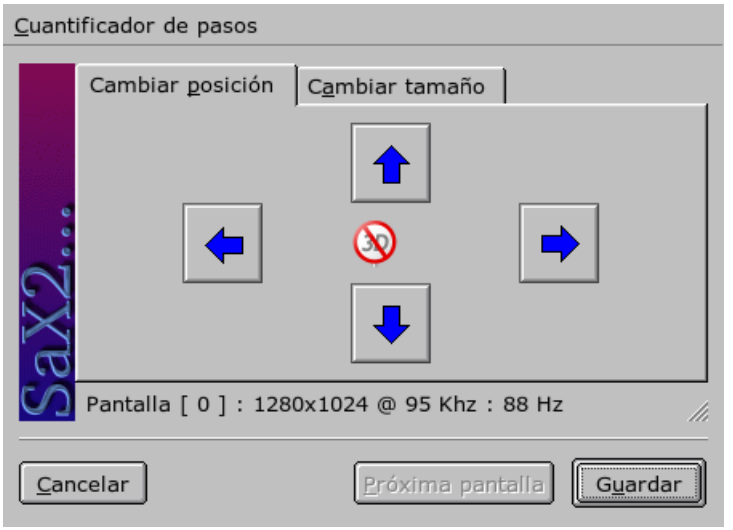

Figura 11.6: *Ajuste de la geometría de la imagen*

11.1.7. Multimonitor

Si tiene más de una tarjeta gráfica en el ordenador o posee una tarjeta gráfica con varias salidas, es posible conectar varios monitores al sistema. El modo de operación con dos monitores se denomina *dualhead* y con más de dos *multihead*. SaX2

detecta automáticamente si existe más de una tarjeta gráfica en el sistema y prepara la configuración en consecuencia. En el diálogo de multimonitor de SaX2 puede definir el modo de trabajo así como el orden de las pantallas. Es posible elegir entre tres modos: 'tradicional' (predeterminado), 'xinerama' y 'clon':

'Multimonitor tradicional' Cada monitor es una unidad en sí misma y el puntero del ratón puede cambiar de una pantalla a otra.

'Multimonitor clon' Este modo se utiliza en presentaciones y ferias y es sobre todo muy efectivo en pantallas del tamaño de una pared. En este modo cada monitor muestra el mismo contenido y el ratón sólo se ve en la ventana principal.

'Multimonitor xinerama' Todas las pantallas se fusionan en una sola pantalla grande. Las ventanas de los programas pueden colocarse libremente en todos los monitores o modificar su tamaño para que ocupe más de un monitor.

Por esquema de pantalla de un entorno multimonitor se entiende el orden y las relaciones de comportamiento entre las distintas pantallas. Por defecto, SaX2 configura un esquema de pantalla estándar que sigue el orden de las tarjetas gráficas detectadas y coloca todas las pantallas en una línea de izquierda a derecha. En el diálogo 'Distribución' de la herramienta multimonitor puede determinar muy fácilmente el orden de los monitores en el escritorio desplazando los símbolos de pantalla en la malla por medio del ratón. Una vez cerrado el diálogo de distribución, puede comprobar la nueva configuración con el botón 'Prueba'.

Tenga en cuenta que en la actualidad Linux no ofrece aceleración 3D para un entorno multimonitor xinerama. En este caso SaX2 desactivará el soporte 3D.

11.1.8. Dispositivos de entrada

Ratón Si la detección automática no reconoce el ratón, configúrelo de forma manual con este diálogo. Puede consultar el modelo y la descripción del ratón en la documentación del mismo. Escoja el valor correspondiente de la lista de modelos de ratón soportados. Después de haber marcado el modelo adecuado, confirme la selección pulsando sobre la tecla ⑤ del bloque numérico.

Teclado En el campo de selección de este diálogo puede determinar el tipo de teclado que utiliza. Debajo puede escoger el idioma de la distribución del

teclado. Finalmente, el apartado para pruebas le permite comprobar si se ha elegido la disposición lingüística correcta; para ello introduzca signos especiales del idioma escogido.

El estado de la casilla utilizada para la activación o desactivación de las letras acentuadas depende del lenguaje seleccionado y no debe modificarse. Pulse en 'Finalizar' para que los cambios tengan efecto.

Pantalla táctil En la actualidad X.Org soporta pantallas táctiles de las marcas Microtouch y Elographics. En este caso SaX2 puede reconocer el monitor automáticamente, pero no el lápiz. El lápiz se puede considerar un dispositivo de entrada.

Para configurarlo correctamente, inicie SaX2 y escoja 'Dispositivos de entrada' → 'Pantalla táctil'. Pulse en 'Añadir...' para agregar una pantalla táctil y guarde la configuración pulsando en 'Finalizar'. No es necesario probar la configuración.

Las pantallas táctiles disponen de una gran variedad de opciones que se deben calibrar primero en la mayoría de los casos. Lamentablemente, en Linux no existe ninguna herramienta adecuada para este fin. No obstante, la configuración estándar contiene valores predeterminados adecuados al tamaño de las pantallas táctiles, por lo que no deberá realizar ninguna configuración adicional.

Tabletas gráficas En la actualidad, X.Org soporta solamente algunas tabletas gráficas. SaX2 permite la configuración de tabletas gráficas conectadas al puerto serie o USB. A efectos de la configuración, una tableta gráfica es un dispositivo de entrada más como por ejemplo un ratón.

Inicie SaX2 y escoja 'Dispositivos de entrada' → 'Tableta gráfica'. Pulse en 'Añadir', seleccione el fabricante en el siguiente diálogo y añada la tableta gráfica de la lista ofrecida. Active las casillas de la derecha si tiene un lápiz o una goma conectados. Si la tableta está conectada al puerto serie, compruebe el puerto: `/dev/ttyS0` indica el primer puerto serie, `/dev/ttyS1` el segundo, etc. Pulse en 'Finalizar' para guardar la configuración.

11.1.9. AccessX

Si desea trabajar sin ratón, inicie SaX2 y active AccessX en el apartado 'Control de acceso'. De esta forma, podrá controlar los movimientos del puntero del ratón en la pantalla con el bloque de teclas numéricas del teclado. En la tabla **??** en esta página puede consultar una descripción de las funciones de las distintas teclas.

Cuadro 11.1: *AccessX: control del ratón con el bloque numérico*

Tecla	Descripción
(÷)	Activa el botón izquierdo del ratón.
(×)	Activa el botón central del ratón.
(−)	Activa el botón derecho del ratón.
(5)	Esta tecla reproduce la pulsación del botón del ratón previamente activado. Si no hay ningún botón activado, se utilizará el botón izquierdo. La activación de la tecla correspondiente volverá a la configuración predeterminada una vez realizado el clic.
(+)	Esta tecla tiene el mismo efecto que la tecla (5) con la diferencia de que ejecuta un doble clic.
(0)	Esta tecla tiene el mismo efecto que la tecla (5) con la diferencia de que mantiene el botón pulsado.
(Supr)	Esta tecla libera la pulsación del botón del ratón provocada por la tecla (0).
(7)	Mueve el ratón hacia arriba a la izquierda.
(8)	Mueve el ratón hacia arriba en línea recta.
(9)	Mueve el ratón hacia arriba a la derecha.
(4)	Mueve el ratón hacia la izquierda.
(6)	Mueve el ratón hacia la derecha.
(1)	Mueve el ratón hacia abajo a la izquierda.
(2)	Mueve el ratón hacia abajo en línea recta.
(3)	Mueve el ratón hacia abajo a la derecha.

11.1.10. Joystick

Aunque es un dispositivo de entrada, el joystick no se configura en SaX sino en el módulo de YaST 'Hardware''Joystick'. Para configurarlo, seleccione en la lista el fabricante y modelo adecuados. Con 'Probar' puede comprobar si el joystick funciona correctamente. El diálogo de prueba muestra tres diagramas para los ejes

análogos del joystick y marcas para los cuatro botones estándar. Si mueve el joystick o pulsa los botones, debería observar algún tipo de reacción en la ventana de diálogo. Puesto que la mayoría de los joysticks están conectados a tarjetas de sonido, también puede acceder a este módulo desde la configuración de la tarjeta de sonido.

11.1.11. Información adicional

Puede encontrar más información sobre el sistema X Windows y sus propiedades en el capítulo ?? en esta página.

11.2. Optimizar la configuración de X Window

X.Org es una implementación de código abierto del sistema X Window desarrollada por la X.Org Foundation. Esta organización también se encarga de desarrollar nuevas tecnologías y estándares para el sistema X Window.

Para poder utilizar el hardware existente (ratón, tarjeta gráfica, monitor, teclado) de la mejor manera posible, se puede optimizar la configuración de forma manual. A continuación se discutirán algunos aspectos de esta optimización manual. Puede encontrar información detallada sobre la configuración del sistema X Window en diversos archivos del directorio `/usr/share/doc/packages/Xorg` así como en la página man `man xorg.conf`.

Aviso

Se recomienda mucha precaución a la hora de configurar el sistema X Window. Jamás se debe arrancar X11 sin haber terminado la configuración. Un sistema mal configurado puede ocasionar daños irreparables en el hardware; los monitores de frecuencia fija corren un riesgo especial. Los autores de este libro y SUSE LINUX no se responsabilizan de posibles daños. El presente texto fue redactado con el máximo cuidado; no obstante, no se puede garantizar que lo métodos presentados sean correctos para su hardware ni que no puedan causarles daño.

Aviso

Los programas SaX2 y xf86config generan el archivo `xorg.conf` y lo copian generalmente en el directorio `/etc/X11`. Este es el archivo de configuración principal del X Window System que contiene las definiciones de ratón, monitor y tarjeta de vídeo.

A continuación se describe la estructura del archivo de configuración `/etc/X11/xorg.conf`. Este archivo se divide en secciones (sections) que comienzan con la palabra clave `Section "nombre"` y terminan con `EndSection`. Estas secciones se explican a grandes rasgos en los siguientes apartados.

`xorg.conf` se compone de varios párrafos llamados secciones (sections) y cada una contempla un determinado aspecto de la configuración. Cada sección tiene la estructura:

```
Section "Nombre"
  definición 1
  definición 2
  definición n
EndSection
```

Existen los siguientes tipos de secciones:

Cuadro 11.2: *Secciones en /etc/X11/xorg.conf*

Tipo	Significado
`Files`	Esta sección describe las rutas para los juegos de caracteres y la tabla de colores RGB.
`ServerFlags`	Aquí se apuntan indicadores generales (flags).
`InputDevice`	Esta es la sección de configuración de los dispositivos de entrada. Se configuran tanto teclados y ratones como dispositivos de entrada especiales tales como joysticks, tabletas digitalizadoras, etc. Las variables importantes aquí son `Driver` y las opciones `Protocol` y `Device` para determinar el protocolo y el dispositivo.

`Monitor`	Descripción del monitor usado. Los elementos de esta sección son un nombre que se utilizará más adelante como referencia en la definición de la pantalla (`Screen`), así como el valor de la anchura de banda (`Bandwidth [MHz]`) y de las frecuencias de sincronización permitidas (`HorizSync [kHz]` y `VertRefresh [Hz]`). El servidor rechaza cualquier modeline que no cumpla con la especificación del monitor; de esta forma se evita enviar al monitor por error frecuencias demasiado altas cuando se está experimentando con los modelines.
`Modes`	Aquí se definen los parámetros para las determinadas resoluciones de pantalla. SaX2 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 por ejemplo en caso de usar un monitor con frecuencia fija. La explicación exacta de todos los parámetros se encuentra en el archivo HOWTO `/usr/share/doc/howto/en/XFree86-Video-Timings-HOWTO.gz`.
`Device`	Esta sección define una determinada tarjeta gráfica cuya referencia es el nombre que aparece por detrás de la palabra clave `Device`.
`Screen`	Esta sección une finalmente un `Monitor` con un `Device` para formar así las indicaciones necesarias para X.Org. La subsección `Display` permite la definición de un tamaño de pantalla virtual (`Virtual`), del `ViewPort` y de los `Modes` usados con este `Screen`.
`ServerLayout`	Esta sección define el diseño de una configuración con uno o varios monitores (”single” o ”multihead”). Los dispositivos de entrada `InputDevice` y los monitores `Screen` se unen para formar un conjunto.

A continuación se contemplan más de cerca las secciones `Monitor`, `Device` y `Screen`. En las páginas del manual relativas a `X.Org` y `xorg.conf` encontrará información adicional sobre el resto de secciones.

El archivo `xorg.conf` puede contener varias secciones de tipo `Monitor` y `Device`. También pueden aparecer diversas secciones `Screen`. De la siguiente sección `ServerLayout` depende cuál de ellas se va a utilizar.

11.2.1. Sección Screen

Primero queremos profundizar un poco más en la sección `Screen`. Esta une una sección de Monitor y de Device y determina qué resolución debe utilizarse con qué profundidad de color. Una sección del tipo Screen puede parecerse, por ejemplo, al ejemplo **??** en esta página.

Ejemplo 11.1: *La sección Screen del archivo /etc/X11/xorg.conf*

```
Section "Screen"
  DefaultDepth  16
  SubSection "Display"
    Depth       16
    Modes       "1152x864" "1024x768" "800x600"
    Virtual     1152x864
  EndSubSection
  SubSection "Display"
    Depth       24
    Modes       "1280x1024"
  EndSubSection
  SubSection "Display"
    Depth       32
    Modes "640x480"
  EndSubSection
  SubSection "Display"
    Depth        8
    Modes       "1280x1024"
  EndSubSection
  Device        "Device[0]"
  Identifier    "Screen[0]"
  Monitor       "Monitor[0]"
EndSection
```

La línea `Identifier` (en este ejemplo el identificador es `Screen[0]`) da un nombre único a la sección para poder identificarla 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 (identifiers). Estas secciones se explican más adelante.

La variable `DefaultDepth` indica la profundidad de color por defecto que usa el servidor cuando arranca sin definición explícita de ella. A cada profundidad de color le sigue 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. No todos los módulos de servidor X soportan todos los valores.

Después de definir la profundidad de color se define una lista de resoluciones con `Modes`. El servidor X lee esta lista de izquierda a derecha. Para cada una de las resoluciones listadas, el servidor busca en la sección `Modes` un `Modeline` que pueda ser representada por el monitor y la tarjeta gráfica.

La primera resolución adecuada en este sentido es la que usa el servidor X para arrancar (`Default-Mode`). Con las teclas Ctrl-Alt-gris + se puede navegar en la lista de resoluciones a la derecha y con Ctrl-Alt-gris - a la izquierda. Gris indica aquí que se trata de teclas del bloque numérico, ya que estas se resaltan a veces en color gris. 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. Ya que 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 por ejemplo 16 MB Vídeo RAM, la pantalla virtual puede ser de hasta 4096x4096(!) puntos con 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.

11.2.2. Sección Device

Una sección de dispositivo (Device-Section), describe una determinada tarjeta gráfica. `xorg.conf` puede incluir una cantidad infinita de secciones de dispositivo siempre que sus nombres, indicados con la palabra clave `Identifier`, se distingan. 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 archivo muestra el extracto de una

sección del tipo `Device` de un ordenador con una tarjeta PCI tipo Matrox Millennium:

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

La sección `Device` debería ser semejante a la que se muestra arriba si se usa SaX2 para la configuración. SaX2 determina automáticamente `Driver` y `BusID`, los cuales dependen del hardware integrado en su máquina. `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 son hexadecimales.

En el parámetro `Driver` se determina el controlador para la tarjeta gráfica, que en el caso de la Matrox Millennium es `mga`. El servidor X busca el controlador 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 controlador se obtiene añadiendo `_drv.o` al identificador, lo que resulta en nuestro ejemplo en `mga_drv.o`.

Existen opciones adicionales para activar ciertas características del servidor X y de su controlador. 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 controlador usado, hay diferentes opciones que se explican junto con los controladores en el directorio `/usr/X11R6/lib/X11/doc`. También puede encontrar opciones generales en las páginas del manual `man xorg.conf` y `man X.Org`.

11.2.3. 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 archivo de configuración `/etc/X11/xorg.conf`. En la sección de ServerLayout se determina qué sección de monitor es relevante 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 (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 averías en el monitor.

Aviso

A quienes deseen desarrollar sus propias descripciones de monitor se les recomienda encarecidamente consultar la documentación disponible en `/usr/X11/lib/X11/doc`. Mención especial merece la sección dedicada a los modos de video, donde se describe de forma detallada el funcionamiento del hardware y la creación de Modelines.

Por fortuna, hoy en día casi nunca hace falta generar Modelines o definiciones de monitores manualmente. Si dispone de un monitor de multifrecuencia moderno, SaX2 puede leer vía DDC los rangos de frecuencia admitidas y las resoluciones óptimas directamente del 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.

11.3. Instalación y configuración de tipos de letra

Instalar tipos de letra adicionales en SUSE LINUX resulta muy sencillo. Basta con copiar los tipos de letra en un directorio especificado en la ruta de tipos de letra de X11 (véase la sección **??** en esta página). Con el fin de que los tipos de letra también puedan utilizarse con el nuevo sistema de representación de tipos de letra xft, este directorio ha de ser además un subdirectorio de los directorios configurados en `/etc/fonts/fonts.conf` (véase la sección **??** en esta página).

Puede copiar los archivos de tipo de letra como usuario `root` en un directorio adecuado como por ejemplo `/usr/X11R6/lib/X11/fonts/truetype`, o bien

utilizar el instalador de tipos de letra de KDE en el centro de control de KDE. El resultado es el mismo.

En lugar de copiar realmente los tipos de letra, también es posible crear enlaces simbólicos para, por ejemplo, poder utilizar tipos de letra con licencia disponibles en una partición Windows montada. Después de crear el enlace ha de ejecutar `SuSEconfig --module fonts`.

El comando `SuSEconfig --module fonts` activa el script `/usr/sbin/fonts-config`, el cual se ocupa de configurar los tipos de letra. Puede obtener información detallada sobre el funcionamiento de este script en la página del manual correspondiente (`man fonts-config`).

Independientemente del tipo de letra que quiera instalarse, el procedimiento siempre es el mismo. Ya se trate de tipos de letra TrueType/OpenType, de tipo 1 (PostScript) o mapas de bits, todos pueden instalarse en cualquier directorio. Únicamente los tipos de letra CID-keyed suponen una excepción, ver la sección **??** en esta página.

X.Org contiene dos sistemas de tipos de letra completamente distintos: el antiguo sistema *X11 core font* y el de nueva creación *Xft/fontconfig*. A continuación se describirán brevemente ambos sistemas.

11.3.1. Xft

Ya durante la planificación de Xft se prestó una especial atención al soporte de tipos de letra escalables (incluyendo antialiasing). Al contrario de lo que sucede con el sistema X11 core font, cuando se emplea Xft, los tipos de letra son representados por el programa que los utiliza y no por el servidor X. De este modo, el programa en cuestión accede directamente a los archivos de los tipos de letra y obtiene un control absoluto sobre todos los detalles, como por ejemplo la representación de los glifos. Por una parte, sólo así es posible lograr una representación correcta del texto en algunos idiomas. Por otra, el acceso directo a los archivos de tipo de letra resulta muy útil para insertar (embed) tipos de letra para su impresión y lograr así que el documento impreso reproduzca realmente la salida en pantalla.

En SUSE LINUX, los entornos de escritorio KDE y Gnome así como Mozilla y otras muchas aplicaciones utilizan por defecto el sistema Xft. Así pues, Xft ya es utilizado por un número considerablemente mayor de aplicaciones que el antiguo sistema X11 core font.

Xft se sirve de la librería Fontconfig para encontrar los tipos de letra y especificar de qué forma van a ser representados. El comportamiento de fontconfig

se determina mediante un archivo de configuración válido en todo el sistema, `/etc/fonts/fonts.conf`, y otro específico para el usuario: `~/.fonts.conf`. Ambos archivos de configuración de fontconfig deben empezar por

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

y terminar en

```
</fontconfig>
```

Para añadir nuevos directorios en los que deban buscarse tipos de letra, puede insertar líneas como:

```
<dir>/usr/local/share/fonts/</dir>
```

No obstante, esto no suele ser necesario ya que el directorio de usuario `~/.fonts` ya está incluido por defecto en `/etc/fonts/fonts.conf`. Así pues, si un usuario desea instalar tipos de letra adicionales para su uso personal, basta con que las copie en `~/.fonts`.

También puede introducir reglas para definir el aspecto de los tipos de letra, por ejemplo:

```
<match target="font">
 <edit name="antialias" mode="assign">
  <bool>false</bool>
 </edit>
</match>
```

para desactivar el antialiasing para todos los tipos de letra, o bien:

```
<match target="font">
 <test name="family">
  <string>Luxi Mono</string>
  <string>Luxi Sans</string>
 </test>
 <edit name="antialias" mode="assign">
 <bool>false</bool>
 </edit>
</match>
```

para desactivarlo sólo para ciertos tipos de letra.

La mayoría de aplicaciones utilizan por defecto los nombres de tipo de letra `sans-serif` (o su equivalente `sans`), `serif` o `monospace`. Aquí no se trata de nombres de tipos de letra realmente existentes sino de nombres alias que se asignan a un tipo de letra en función del idioma seleccionado.

Todos los usuarios pueden añadir fácilmente reglas a su archivo `~/.fonts.conf` con el fin de que estos nombres alias sean resueltos con determinados tipos de letra:

```
<alias>
 <family>sans-serif</family>
 <prefer>
  <family>FreeSans</family>
 </prefer>
</alias>
<alias>
 <family>serif</family>
 <prefer>
  <family>FreeSerif</family>
 </prefer>
</alias>
<alias>
 <family>monospace</family>
 <prefer>
  <family>FreeMono</family>
 </prefer>
</alias>
```

Debido a que prácticamente todas las aplicaciones utilizan estos nombres alias por defecto, las reglas son válidas para casi todo el sistema. De esta forma y con muy poco esfuerzo, puede utilizar sus tipos de letra preferidos casi siempre sin tener que configurar la opción de tipos de letra en cada programa por separado.

El comando `fc-list` le permite averiguar qué tipos de letra están instalados y disponibles. Así por ejemplo, el comando `fc-list ""` proporciona una lista de todos los tipos de letra. Si desea averiguar qué tipos de letra escalables (`:outline=true`) con todos los glifos necesarios para el hebreo (`:lang=he`) están disponibles así como su denominación (`family`), estilo (`style`), su peso o grosor (`weight`) y el nombre del archivo que contiene el tipo de letra, puede utilizar por ejemplo el siguiente comando:

```
fc-list ":lang=he:outline=true" family style weight file
```

La salida de este comando podría ser la siguiente:

```
/usr/X11R6/lib/X11/fonts/truetype/FreeSansBold.ttf: FreeSans:style=Bold:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeMonoBoldOblique.ttf: FreeMono:style=BoldOblique:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeSerif.ttf: FreeSerif:style=Medium:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeSerifBoldItalic.ttf: FreeSerif:style=BoldItalic:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeSansOblique.ttf: FreeSans:style=Oblique:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeSerifItalic.ttf: FreeSerif:style=Italic:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeMonoOblique.ttf: FreeMono:style=Oblique:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeMono.ttf: FreeMono:style=Medium:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeSans.ttf: FreeSans:style=Medium:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeSerifBold.ttf: FreeSerif:style=Bold:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeSansBoldOblique.ttf: FreeSans:style=BoldOblique:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeMonoBold.ttf: FreeMono:style=Bold:weight=200
```

Los parámetros más importantes que pueden ser consultados con el comando `fc-list` son los siguientes:

Cuadro 11.3: *Parámetros de fc-list*

Parámetro	**Significado y valor posible**
`family`	Nombre de la familia de tipo de letra, por ejemplo `FreeSans`.
`foundry`	Fabricante del tipo de letra, por ejemplo `urw`.
`style`	Estilo del tipo de letra, por ejemplo `Medium`, `Regular`, `Bold`, `Italic`, `Heavy`...
`lang`	Idioma(s) que soporta el tipo de letra. Por ejemplo `es` para el español, `ja` para el japonés, `zh-TW` para el chino tradicional, `zh-CN` para el chino simplificado, etc.
`weight`	El grosor, por ejemplo `80` para no negrita y `200` para negrita.
`slant`	El grado de inclinación, normalmente `0` para no cursiva y `100` para cursiva.
`file`	Nombre del archivo en el que se encuentra el tipo de letra.
`outline`	`true` si se trata de un tipo de letra con contorno, `false` en caso contrario.
`scalable`	`true` si se trata de un tipo de letra escalable, `false` en caso contrario.
`bitmap`	`true` si se trata de un mapa de bit, `false` en caso contrario.
`pixelsize`	Tamaño del tipo de letra en píxeles. En el contexto de fc-list sólo tiene importancia para los mapas de bits.

11.3.2. X11 core fonts

Hoy en día, el sistema X11 core font no sólo soporta mapas de bits sino también tipos de letra escalables como las de tipo 1, TrueType/OpenType y CID-keyed. Los tipos de letra Unicode se soportan también desde hace mucho tiempo. Originalmente, el sistema X11 core font fue desarrollado en 1987 para X11R1 con el fin de procesar tipos de letra de mapas de bit monocromos. Incluso hoy puede observarse que todas las extensiones mencionadas en las líneas superiores han sido añadidas posteriormente.

Por ejemplo, los tipos de letra escalables se soportan exclusivamente sin antialiasing y sin representación de subpíxeles, y el proceso de carga de tipos de letra escalables de grandes dimensiones con glifos para muchos idiomas puede resultar muy lento. Asimismo, el uso de tipos de letra Unicode es en ocasiones también muy lento y consume más memoria.

El sistema X11 Core Font presenta muchos inconvenientes. Se puede argumentar que ha caído en desuso y que no tiene sentido continuar ampliándolo. Aunque debe seguir estando presente por razones de compatibilidad con versiones anteriores, se recomienda utilizar en la medida de lo posible el sistema Xft y fontconfig, mucho más moderno.

Como premisa para su funcionamiento, el servidor X debe conocer tanto los tipos de letras que se encuentran disponibles como su ubicación en el sistema. De ello se ocupa la variable FontPath, la cual engloba la ruta a todos los directorios de tipos de letra válidos del sistema. En cada uno de estos directorios existe un archivo llamado `fonts.dir` que contiene una lista de los tipos de letra disponibles en ese directorio. La variable FontPath, que es generada por el servidor X durante el inicio, busca un archivo `fonts.dir` válido en todas las entradas `FontPath` del archivo de configuración `/etc/X11/xorg.conf`. Dichas entradas se encuentran en la sección `Files`. Puede visualizar el valor actual de FontPath con el comando `xset q`. xset también le permite cambiar esta ruta mientras el sistema está en funcionamiento. Puede añadir una nueva ruta con `xset +fp <ruta>` y eliminarla con `xset -fp <ruta>`.

Una vez que el servidor X está en funcionamiento, es posible activar tipos de letra recién instalados en directorios ya integrados por medio del comando `xset fp rehash`. Este comando es ejecutado por `SuSEconfig --module fonts`.

Debido a que el comando `xset` necesita acceder al servidor X activo, este proceso sólo puede funcionar si `SuSEconfig --module fonts` se activa desde una shell con acceso al servidor X en ejecución. Para ello, el método más sencillo consiste en registrarse en una consola como `root` introduciendo el comando `su` y

la contraseña de root. `sux` transmite los permisos de acceso del usuario que ha iniciado el servidor X a la root shell. Puede utilizar el comando `xlsfonts` para comprobar si los tipos de letra han sido instalados correctamente y si están disponibles por medio del sistema X11 core font. Este comando produce una lista de todos los tipos de letra disponibles.

SUSE LINUX utiliza por defecto locales UTF-8, por lo que normalmente será preferible emplear tipos de letra Unicode. Reconocerá a estos en la lista emitida por `xlsfonts` porque sus nombres terminan en `iso10646-1`. Así pues, para ver una lista de todos los tipos de letra Unicode disponibles, puede servirse del comando `xlsfonts | grep iso10646-1`. La gran mayoría de los tipos de letra Unicode disponibles en SUSE LINUX incluyen al menos todos los glifos necesarios para las lenguas europeas para las que anteriormente se utilizaba la codificación `iso-8859-*`.

11.3.3. Tipos de letra CID-keyed

Al contrario de lo que sucede con otros tipos de letra, en el caso de CID-keyed sí que importa en qué directorio se instala. Este ha de ser siempre `/usr/share/ghostscript/Resource/CIDFont`. Aunque el directorio carezca de importancia para Xft/fontconfig, Ghostscript y el sistema X11 core font requieren que se trate de este directorio en concreto.

Sugerencia

Puede obtener información adicional sobre los tipos de letra en X11 en la URL `http://www.xfree86.org/current/fonts.html`.

Sugerencia

11.4. Configuración 3D de OpenGL

11.4.1. Hardware soportado

SUSE LINUX incluye varios controladores OpenGL para el soporte de hardware 3D. La tabla **??** en esta página le proporciona un resumen de los mismos.

Cuadro 11.4: *Hardware 3D soportado*

Controlador OpenGL	Hardware soportado
nVidia	Chips nVidia: todos excepto Riva 128(ZX)
DRI	3Dfx Voodoo Banshee, 3Dfx Voodoo-3/4/5, Intel i810/i815/i830M, Intel 845G/852GM/855GM/865G,915, Matrox G200/G400/G450/G550, ATI Rage 128(Pro)/Radeon (hasta 9250)

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 es necesario instalar previamente el controlador nVidia. Para ello seleccione durante la instalación el parche del controlador nVidia en YOU (YaST Online Update). Por motivos de licencia no podemos incluir el controlador de nVidia con la distribución.

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.

11.4.2. Controladores OpenGL

Estos controladores OpenGL pueden instalarse muy fácilmente utilizando SaX2. Tenga en cuenta que, si dispone de una tarjeta nVidia, el controlador de nVidia ha de ser instalado previamente como se describe en las líneas superiores. El comando `3Ddiag` le permite comprobar si nVidia 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, que es más lento. Utilice el comando `id` para comprobar si el usuario actual pertenece al grupo `video`. Si este no es el caso, utilice YaST para añadirlo al grupo.

11.4.3. 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 X.Org 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.

11.4.4. Aplicaciones de prueba OpenGL

Para probar OpenGL puede utilizar juegos como `tuxracer` o `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 soporte 3D, esta prueba no tiene sentido (efecto de diapositivas). La salida del comando `glxinfo` le informará de si el soporte 3D está activado. En caso afirmativo, la variable `direct rendering` tendrá el valor `Yes`.

11.4.5. 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 X.Org. A menudo, encontrará aquí la línea `DRI is disabled` en los archivos X.Org `/var/log/Xorg.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.

11.4.6. Soporte de instalación

Excepto el 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.

11.4.7. Documentación adicional en línea

Para ver información sobre DRI, consulte `/usr/X11R6/lib/X11/doc/README.DRI` (paquete `Xorg-x11-doc`). Puede obtener información adicional sobre la instalación de controladores nvidia en `http://ftp.suse.com/pub/suse/i386/supplementary/X/nvidia-installer-HOWTO.html`.

Impresoras

El presente capítulo contiene información general sobre el uso de impresoras, por lo que resultará de gran ayuda a la hora de encontrar soluciones adecuadas para impresoras en redes. El capítulo se concentra de manera especial en el funcionamiento de CUPS e incluye una sección donde se describen los problemas más comunes y los métodos para evitarlos.

12.1. Preparativos y otras consideraciones

CUPS es el sistema de impresión estándar de SUSE LINUX y resulta muy fácil de usar. Generalmente es compatible con LPRng o, por lo menos, no es muy difícil hacer que lo sea. SUSE LINUXSUSE LINUX sólo incorporan LPRng por razones de compatibilidad.

Las impresoras se distinguen básicamente por su interfaz (USB, red) así como por su lenguaje de impresión. Por eso es importante tener en cuenta la compatibilidad de la interfaz y al lenguaje de impresión en el momento de adquirir la impresora. Existen básicamente tres clases diferentes de impresoras atendiendo al lenguaje de impresión:

Impresoras PostScript PostScript es el lenguaje de impresión de Linux/Unix por excelencia para la creación de tareas de impresión y el tratamiento interno. Es un lenguaje muy antiguo y potente. Las fuentes potenciales de errores se reducen si la impresora es capaz de tratar PostScript directamente, ya que se suprimen pasos adicionales de conversión. Debido a las licencias que se han de abonar, las impresoras con intérprete PostScript son normalmente más caras que aquellas que carecen de él.

Lenguajes de impresión estándar como PCL y ESC/P
Se trata de lenguajes de impresión muy antiguos que son constantemente ampliados para cubrir necesidades nuevas. GhostScript es capaz de convertir PostScript en un lenguaje de impresión conocido como PCL, utilizado mayoritariamente en impresoras HP y "clónicos" o en ESC/P, muy extendido entre impresoras Epson. Con estos lenguajes de impresión los resultados bajo Linux suelen ser buenos. Aparte de los controladores `hpijs` desarrollados por HP, actualmente (2004) no existen controladores disponibles bajo licencia OpenSource. Los precios de estas impresoras son de nivel medio.

Impresoras propietarias (normalmente GDI)
Las impresoras propietarias sólo disponen habitualmente de controladores para Windows. No se ha implementado para ellas ningún lenguaje de impresión conocido y el que se utiliza para un modelo determinado puede cambiar de un año a otro. Puede obtener información adicional sobre esta problemática en sección **??** en esta página.

Para consultar el nivel de soporte de una determinada impresora, utilice una de las siguientes fuentes de información antes de adquirirla:

- La base datos de impresoras de SUSE LINUX: `http://cdb.suse.de/`
- La base de datos de impresoras en LinuxPrinting.org: `http://www.linuxprinting.org/`
- La página web de Ghostscript: `http://www.cs.wisc.edu/~ghost/`
- Los controladores incluidos: `file:/usr/share/doc/packages/ghostscript/catalog.devices`

Las bases de datos en línea reflejan sólo el estado actual de soporte Linux y sólo es posible incluir controladores en un producto hasta el momento de su producción. Puede que una impresora con la calificación de "totalmente soportada" todavía no lo estuviera en la fecha de producción de SUSE LINUX. Por tanto, las bases de datos no ofrecen siempre el estado correcto aunque sí al menos una buena aproximación. En la base de datos de impresoras de SUSE LINUX podrá averiguar qué impresoras soporta la versión actual del software.

12.2. Funcionamiento del sistema de impresión

El usuario crea una tarea de impresión. Una tarea de impresión consta de los datos que se van a imprimir más información para el spooler como puede ser el nombre de la impresora, el nombre de la cola de impresión y, opcionalmente, información para el filtro como por ejemplo las opciones específicas de impresora.

Cada impresora dispone de una cola de impresión dedicada. El spooler de impresión retiene la tarea de impresión en la cola hasta que la impresora deseada esté lista para recibir datos. Una vez que la impresora está preparada, el spooler envía los datos a la impresora a través del filtro y el dorsal.

El filtro convierte los datos que el usuario quiere imprimir (ASCII, PostScript, PDF, JPEG, etc.) en datos específicos de impresora (PostScript, PCL, ESC/P, etc.). Las características de la impresora se describen en los archivos PPD. Un archivo PPD contiene las opciones específicas de impresora con los parámetros necesarios para activar dichas opciones en la impresora. El sistema de filtros garantiza que las opciones seleccionadas por el usuario estén activadas.

Si se utiliza una impresora PostScript, el sistema de filtros convierte los datos en PostScript específico de impresora, para lo cual no es necesario ningún controlador de impresora. Si se utiliza una impresora no PostScript, el sistema de filtros convierte los datos en datos específicos de impresora por medio de Ghostscript. Para este proceso se requiere un controlador Ghostscript adecuado para la impresora. El dorsal recibe del filtro los datos específicos de impresora y los pasa a la impresora.

12.3. Integración de impresoras: métodos y protocolos

Existen diferentes posibilidades para conectar una impresora al sistema. Desde el punto de vista de la configuración, en el sistema CUPS no importa si la impresora tiene conexión local o a través de la red. Las impresoras locales se conectan en Linux de acuerdo a las instrucciones de instalación del fabricante. CUPS soporta las siguientes conexiones: puerto serie, USB, puerto paralelo y SCSI. Para obtener información adicional sobre la conexión de impresoras, consulte el artículo *CUPS in a Nutshell* de la base de datos de soporte `http://portal.suse.com`, al que puede acceder introduciendo el término de búsqueda *cups*.

Aviso

Conexión por cable al ordenador

Sólo las conexiones del tipo USB están diseñadas para ser conectadas ”en caliente”. Las demás conexiones sólo deben ser modificadas cuando todo esté apagado.

Aviso

12.4. Instalación del software

”PostScript Printer Description” (PPD) es el lenguaje que describe las propiedades (ej. resolución) y opciones (ej. impresión doble cara) de las impresoras. CUPS necesita estas descripciones para poder utilizar las prestaciones de la impresora. Si no existe ningún archivo PPD, los datos se envían a la impresora en formato ”crudo”, lo que habitualmente no es lo deseado. SUSE LINUX incluye muchos archivos PPD para permitir el uso de las impresoras que no soporten PostScript.

Si se ha configurado una impresora PostScript se recomienda obtener el archivo PPD correspondiente. Muchos de estos PPDs se encuentran en el paquete `manufacturer-PPDs` incluido en la instalación estándar. Vea también sección **??** en esta página y sección **??** en esta página.

Los archivos PPD nuevos se han de guardar en el directorio `/usr/share/cups/model/` o mejor se añaden al sistema de impresión por medio de YaST (ver sección Configuración manual en esta página). A continuación será posible seleccionar el archivo PPD durante la instalación.

Hay que tener cuidado cuando el fabricante de la impresora no sólo requiere que se modifiquen los archivos de configuración sino también la instalación de paquetes enteros de software. Al realizar tal instalación se pierde por una parte el derecho al servicio de soporte de SUSE LINUX y, por otra, es posible que ciertos comandos de impresión funcionen de forma diferente a la habitual o que dispositivos de otros fabricantes dejen de funcionar completamente. Por este motivo no se recomienda instalar software del fabricante.

12.5. Configuración de la impresora

Después de conectar la impresora con el ordenador e instalar el software, hace falta instalar la impresora en el sistema. Utilice con este fin las herramientas incluidas en SUSE LINUX. En SUSE LINUX la seguridad juega siempre un papel principal, por lo que las herramientas de terceros no siempre son capaces de manejar las restricciones de seguridad del sistema y a veces pueden provocar más problemas que soluciones.

12.5.1. Impresora local

Si al iniciar el sistema se detecta una impresora sin configurar, se iniciará automáticamente un módulo de YaST para configurarla. A continuación se describen los diálogos y el proceso de configuración.

Dentro del centro de control de YaST, seleccione 'Hardware' → 'Impresora' para que aparezca la ventana principal de la configuración de impresora. La parte superior muestra las impresoras detectadas y la inferior las colas configuradas. Las impresoras que no han sido detectadas automáticamente pueden configurarse manualmente.

Importante

Si no encuentra la entrada 'Impresora' en el centro de control de YaST, lo más probable es que el paquetes `yast2-printer` no esté instalado. Para resolver este problema, instale dicho paquete y reinicie YaST.

Importante

Configuración automática

YaST permite la configuración automática de la impresora siempre y cuando el puerto paralelo o USB se configure automáticamente y la impresora conectada al puerto se detecte correctamente. La base de datos de impresoras contiene la identificación del modelo de impresora que YaST recibió al detectarla. En caso de que esta identificación "electrónica" sea diferente a la denominación comercial, deberá seleccionar la impresora manualmente.

Utilice la impresión de prueba de YaST después de cualquier configuración para comprobar que todo funciona correctamente. La hoja de prueba de YaST muestra también información importante sobre la configuración que se está probando.

Configuración manual

La configuración de la impresora debe realizarse manualmente si alguna de las condiciones para la detección automática no se cumple o si desea realizar una configuración individual. Dependiendo del nivel de detección de hardware y de la cantidad de información disponible sobre una impresora en la base de datos de impresoras, YaST puede averiguar automáticamente los datos necesarios y ofrecer una preselección adecuada.

Es necesario configurar los siguientes parámetros:

Interfaz de conexión (puerto) La configuración de la interfaz de conexión depende de la detección automática de la impresora por parte de YaST. Si YaST es capaz de detectar la impresora automáticamente, se puede suponer que la conexión a la impresora funciona y que no se necesita más ajustes. Al contrario, si YaST no fuera capaz de detectar el modelo de impresora automáticamente, es muy probable que la conexión a la impresora a nivel de hardware no llegue a funcionar sin configuración manual.

Nombre de la cola de impresión El nombre de la cola se utiliza para introducir comandos de impresión. Se recomienda emplear un nombre corto compuesto sólo por minúsculas y números.

Modelo de impresora y archivo PPD Los parámetros específicos de impresora como por ejemplo el controlador Ghostscript que se debe utilizar y los parámetros de filtrado para el controlador, se guardan en un archivo del tipo PPD (PostScript Printer Description). Puede obtener información adicional sobre los archivos PPD en sección **??** en esta página.

Existen muchas impresoras que disponen de varios archivos PPD (ej. cuando varios controladores GhostScript funcionan con esa impresora). Al seleccionar el fabricante y modelo YaST muestra en primer lugar los archivos PPD que corresponden a la impresora. Si existen varios archivos PPD, YaST selecciona aquel calificado como `recommended`. Si es necesario puede pulsar 'Modificar' para seleccionar otro archivo PPD.

En el caso de las impresoras que no entienden PostScript, el controlador Ghostscript se encarga de producir todos los datos específicos de impresora. Por este motivo, la configuración de este controlador es el punto clave para determinar la calidad de la impresión. La impresión final es el resultado del tipo de controlador Ghostscript seleccionado (archivo PPD) y de las opciones especificadas para el mismo. En caso de necesidad es posible cambiar opciones adicionales (si están disponibles en el archivo PPD) pulsando 'Modificar'.

La impresión de la hoja de prueba es imprescindible para comprobar si la configuración seleccionada funciona correctamente. Si la impresión de esta hoja fuera errónea (por ejemplo porque se imprimen muchas hojas casi vacías), puede detener el proceso de impresión retirando el papel de la impresora y cancelando a continuación la impresión de prueba de YaST.

Si el modelo de impresora no se encuentra dentro de la base de datos de impresoras, puede añadir un nuevo archivo PPD mediante la opción 'Añadir archivo PPD a la base de datos' o bien seleccionar uno de los archivos PPD genéricos para los lenguajes de impresión estándar. Para ello escoja 'UNKNOWN MANUFACTURER' como fabricante.

Configuración avanzada Normalmente no es necesario configurar nada más.

Configuración de la impresora con herramientas de línea de comandos

Para configurar manualmente la impresora con herramientas de línea de comandos (ver sección Configuración en la línea de comandos en esta página), necesitará una URI (Uniform Resource Identifier) de dispositivo formada por un dorsal como por ejemplo usb y parámetros como /dev/usb/lp1. Un ejemplo de URI

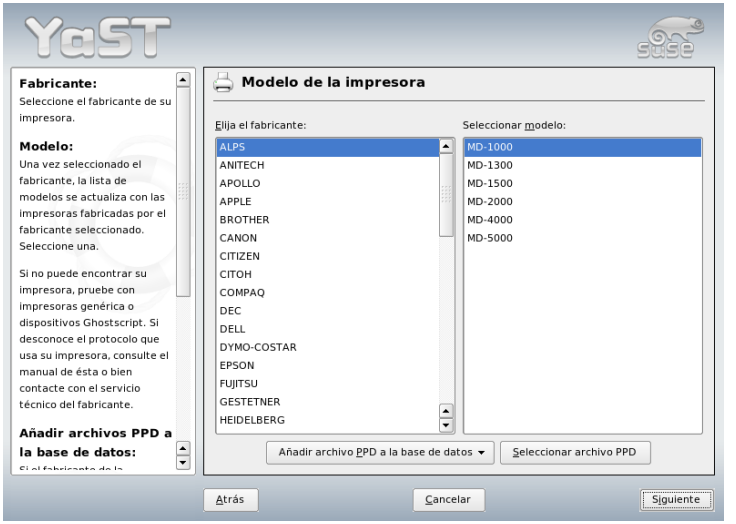

Figura 12.1: *Selección del modelo de impresora*

puede ser `parallel:/dev/lp0` (impresora conectada al primer puerto paralelo) o `usb:/dev/usb/lp0` (primera impresora detectada conectada al puerto USB).

12.5.2. Impresoras de red

Las impresoras de red funcionan con diferentes protocolos, algunas de ellas con varios simultáneamente. La mayoría de estos protocolos son estandarizados. Sin embargo, a veces los fabricantes amplían y modifican el estándar por no haberlo implementado correctamente o por añadir ciertas funciones que no existen en el estándar. Este tipo de controladores sólo existe para unos pocos sistemas operativos entre los que no se suele encontrar Linux. Dado que no se puede garantizar el funcionamiento correcto de todos los protocolos, es recomendable probar diferentes posibilidades para alcanzar una configuración correcta.

CUPS soporta los protocolos `socket`, `LPD`, `IPP` y `smb`, que se explican a continuación:

socket "socket" denomina una conexión que manda los datos sobre un

Socket de Internet sin que se haya realizado previamente un intercambio (handshake) de datos. Los puertos de socket típicos son `9100` o `35`. Ejemplo para una denominación de dispositivo del tipo URI: `socket://host-printer:9100/`

LPD (Line Printer Daemon) El protocolo LPD tiene una larga tradición. LPD significa "Line Printer Daemon" y se explica en RFC 1179. El protocolo define el envío de algunos datos administrativos (ej. ID de la cola de impresión) antes de los datos reales. Por eso hace falta indicar una cola de impresión para configurar LPD. Las implementaciones de muchos fabricantes aceptan casi cualquier nombre. En caso de duda consulte el manual de la impresora; los nombres suelen ser LPT, LPT1, LP1 o algo parecido. El mismo procedimiento permite configurar una cola LPD en otro ordenador Linux o Unix con el sistema CUPS. El número de puerto para el servicio LPD es `515`. Un ejemplo de nombre de dispositivo URI es: `lpd://host-printer/LPT1`

IPP (Internet Printing Protocol) El protocolo IPP es aún relativamente joven (1999) y está basado en el protocolo HTTP. Este protocolo envía muchos más datos relacionados con la tarea de impresión que otros protocolos. CUPS lo utiliza para el tratamiento interno de datos. Al configurar una cola de reenvío (forwarding queue) entre dos servidores CUPS se recomienda utilizar este protocolo. Igualmente, para configurar IPP correctamente se necesita el nombre de la cola de impresión. El número de puerto para IPP es `631`. Ejemplo de un nombre de dispositivo URI: `ipp://host-printer/ps` o bien: `ipp://host-cupsserver/printers/ps`

SMB (recurso compartido de Windows)
CUPS soporta también la impresión en una impresora compartida de Windows. El protocolo utilizado se llama SMB y se utilizan los puertos `137`, `138` y `139`. Ejemplo de un nombre de dispositivo URI: `smb://user:password@workgroup/server/printer` o bien: `smb://user:password@host/printer` o bien: `smb://server/printer`

Antes de instalar una impresora, hay que averiguar qué protocolo soporta. Si el fabricante no proporciona esta información, existe la posibilidad de "adivinarlo" con el comando `nmap` incluido en el paquete `nmap`. `nmap` averigua los puertos abiertos, por ejemplo:

```
nmap -p 35,137-139,515,631,9100-10000 printerIP
```

12.5.3. Tareas de configuración

Las tareas de configuración pueden llevarse a cabo por medio de YaST o a desde la lína de comandos.

Configuración de CUPS con YaST en la red

Las impresoras en la red han de configurarse con YaST ya que, además de facilitar la configuración, YaST resulta muy adecuado para manejar las restricciones de seguridad de CUPS (ver sección **??** en esta página).

Puede consultar una guía práctica de configuración de "CUPS en la red" en el artículo *CUPS in a Nutshell* de la base de datos de soporte `http://portal.suse.com`. Para acceder a este artículo, introduzca el término de búsqueda *cups*.

Configuración en la línea de comandos

Existe la posibilidad de configurar CUPS con herramientas de la línea de comandos como `lpadmin` y `lpoptions`. Una vez completados los preparativos (conocer el archivo PPD y el nombre URI de dispositivo), se llevan a cabo los siguientes pasos:

```
lpadmin -p queue -v device-URI \
-P PPD-file -E
```

Es importante que la primera opción no sea `-E`, ya que todos los comandos CUPS interpretan la opción `-E` en primera posición como solicitud para una conexión codificada (en inglés encrypted). La intención de la opción `-E` en el ejemplo superior es la de activar (enable) la impresora. Un ejemplo concreto:

```
lpadmin -p ps -v parallel:/dev/lp0 \
  -P /usr/share/cups/model/Postscript.ppd.gz -E
```

Ejemplo para configurar una impresora de red:

```
lpadmin -p ps -v socket://192.168.1.0:9100/ \
  -P /usr/share/cups/model/Postscript-level1.ppd.gz -E
```

Modificar opciones

Aunque durante la instalación del sistema se definen ciertas opciones como opciones predeterminadas, es posible modificar estas opciones para cada tarea de impresión (en función de la herramienta de impresión utilizada). Las opciones predeterminadas pueden cambiarse con YaST o bien desde la línea de comandos. Con herramientas de la línea de comandos, se realiza de la siguiente forma:

1. Primero mostrar una lista de todas las opciones:

   ```
   lpoptions -p queue -l
   ```

   Ejemplo:

   ```
   Resolution/Output Resolution: 150dpi *300dpi 600dpi
   ```

   El asterisco precede a la opción activada por defecto: `*`

2. Modificar una opción con `lpadmin`:

   ```
   lpadmin -p queue -o Resolution=600dpi
   ```

3. Comprobar que la opción se ha fijado correctamente:

   ```
   lpoptions -p queue -l
   ```

   ```
   Resolution/Output Resolution: 150dpi 300dpi *600dpi
   ```

12.6. Configuración de las aplicaciones

Las aplicaciones utilizan las colas de impresión de forma análoga a la impresión desde la línea de comandos. Utilice sencillamente las colas de impresión existentes en lugar de configurar la impresora nuevamente desde la aplicación.

12.6.1. Imprimir desde la línea de comandos

Para imprimir desde la línea de comandos se utiliza el comando `lp -d` ⟨*`cola`*⟩ ⟨*`nombre_archivo`*⟩. Tenga en cuenta que ⟨*cola*⟩ y ⟨*nombre_archivo*⟩ han de sustituirse por los valores reales.

12.6.2. Imprimir a través de la línea de comandos en aplicaciones

Algunas aplicaciones utilizan el comando `lp` para imprimir. En la máscara de impresión de la aplicación introduzca el comando de impresión adecuado (normalmente sin especificar el ⟨*nombre_archivo*⟩). Por ejemplo: `lp -d` ⟨*cola*⟩. Para poder introducir un comando de impresión dentro del diálogo de impresión de KDE hay que cambiarlo a 'Imprime a través de un sistema externo'.

12.6.3. Imprimir a través de CUPS

Algunas herramientas como xpp o el programa de KDE kprinter disponen de menús gráficos para seleccionar las colas de impresión y definir las opciones estándar de CUPS y otras opciones de impresión específicas de los archivos PPD. Para utilizar kprinter como interfaz estándar de impresión también para aplicaciones que no pertenezcan a KDE, introduzca dentro de la máscara de impresión de la aplicación el comando `kprinter` o `kprinter --stdin`. Dependiendo de la aplicación en cuestión, deberá utilizar el comando con o sin la opción `--stdin`. Si esto se ha realizado correctamente, cada vez que se origine una tarea de impresión, la aplicación activará el diálogo de kprinter para que pueda ajustar la cola de impresión y otras opciones. Para ello es necesario que la configuración de la máscara de impresión de la aplicación no entre en conflicto con la configuración de kprinter y que las opciones de impresión pasen a configurarse exclusivamente con kprinter una vez que este haya sido activado.

12.7. Particularidades en SUSE LINUX

CUPS se ha modificado en algunos aspectos para un mejor funcionamiento con SUSE LINUX. A continuación se explican las modificaciones más importantes:

12.7.1. El servidor CUPS y el cortafuegos

Existen numerosos métodos para configurar CUPS como cliente de un servidor de red.

- Se pueden crear colas locales para cada cola del servidor de red y utilizarlas para enviar los trabajos de impresión a la cola respectiva del servidor de

red. Este método no es recomendable ya que si se modifica la configuración del servidor de red, será necesario volver a configurar todos los clientes.

- También es posible reenviar los trabajos de impresión a un solo servidor de red. Para esta configuración no es necesario que se ejecute el daemon CUPS; `lpr` (o librerías equivalentes activadas por otros programas) puede enviar trabajos de impresión directamente al servidor de red. No obstante, este tipo de configuración no funciona si se quiere imprimir en una impresora conectada localmente.
- Otro método consiste en estar a la escucha de paquetes broadcast IPP. El daemon CUPS puede escuchar este tipo de paquetes enviados por otros servidores de red para anunciar las colas de impresión disponibles. Esta es la configuración de CUPS más adecuada para imprimir a través de un servidor CUPS remoto. No obstante, con esta configuración también se corre el riesgo de que un agresor envíe al daemon paquetes broadcast IPP con sus colas y de que estas colas estén disponibles a través del daemon local. Si el daemon anuncia una de estas colas con el mismo nombre que otra cola del servidor local y el paquete IPP se ha recibido antes, los trabajos de impresión serán enviados al servidor del agresor en lugar de al servidor local sin que el usuario se aperciba de ello. Esta configuración requiere que el puerto UDP 631 esté abierto para paquetes entrantes.

Para detectar un servidor CUPS, YaST puede sondear ("scan") todos los equipos de una red red para ver si ofrecen este servicio, o bien estar a la escucha de paquetes broadcast IPP (siguiendo el principio descrito en las líneas superiores). Este método también se utiliza durante la instalación para detectar un servidor CUPS para la propuesta de instalación. El segundo método requiere que el puerto UDP 631 esté abierto para paquetes entrantes.

En cuanto al cortafuegos, está preconfigurado (conforme a la propuesta) de tal forma que *no* acepta los broadcasts IPP en ninguna interfaz. Esto significa que tanto el segundo método para detectar un servidor CUPS como el tercer método para acceder a colas de impresión remotas no pueden funcionar. Para que funcionen es necesario modificar la configuración del cortafuegos, bien marcando una interfaz como `interna` para que el puerto esté abierto por defecto, bien abriendo explícitamente el puerto de las interfaces `externas`. Ninguna de estas opciones puede estar activada por defecto por razones de seguridad. La apertura del puerto exclusivamente a efectos de detección (para configurar el acceso remoto a las colas conforme al segundo método) constituye también un problema de seguridad: los usuarios podrían no leer la propuesta y aceptar el servidor de un agresor externo.

Resumiendo, el usuario debe modificar la propuesta de configuración del cortafuegos para permitir a CUPS detectar colas remotas durante la instalación y posteriormente acceder a las colas remotas de múltiples servidores en la red local. Como alternativa, el usuario puede sondear los ordenadores de la red para detectar un servidor CUPS o bien configurar todas las colas manualmente (lo cual no se recomienda por las razones mencionadas arriba).

12.7.2. Administración con el frontal web de CUPS

Para poder utilizar la administración con el frontal web de CUPS o la herramienta de administración de impresoras de KDE, es necesario configurar al usuario `root` como administrador de CUPS con el grupo de administración `sys` y una contraseña para CUPS. Esto se lleva a cabo ejecutando el siguiente comando como `root`:

```
lppasswd -g sys -a root
```

En caso contrario no es posible llevar a cabo la administración a través de la web porque la autentificación falla si no se ha configurado ningún administrador de CUPS. En lugar de `root`, otro usuario puede figurar como administrador de CUPS; vea a este respecto la sección **??** en esta página .

12.7.3. Cambios en el sistema de impresión CUPS (cupsd)

Los siguientes cambios fueron introducidos a partir de SUSE LINUX 9.1.

cupsd se ejecuta como usuario lp

Después de iniciarse, `cupsd` cambia del usuario `root` a `lp`. Esto incrementa la seguridad ya que el servicio de impresión de CUPS ya no se ejecuta con derechos ilimitados sino sólo con los derechos necesarios para el servicio de impresión.

La desventaja de este cambio radica en que ya no es posible realizar la autentificación (para ser más exacto, la comprobación de la contraseña) mediante `/etc/shadow` porque `lp` no tiene acceso a este archivo. En su lugar debe utilizarse la autentificación específica de CUPS vía `/etc/cups/passwd.md5`. Para ello es preciso dar de alta un administrador de CUPS con el grupo de administración `sys` y una contraseña de CUPS dentro de `/etc/cups/passwd.md5`. Ejecute el siguiente comando como `root`:

```
lppasswd -g sys -a CUPS-admin-name
```

Cuando `cupsd` se ejecuta como `lp`, no es posible crear `/etc/printcap` ya que `lp` no puede crear archivos dentro del directorio /etc/. Por eso cupsd crea `/etc/cups/printcap`. Además se genera un enlace simbólico `/etc/printcap` que apunta a `/etc/cups/printcap`.

Después de ejecutar cupsd como `lp` ya no se puede abrir el puerto 631. Esto hace que resulte imposible volver a cargar cupsd mediante el comando `rccups reload`. En lugar de ello se puede utilizar `rccups restart`.

Funcionalidad general de BrowseAllow y BrowseDeny

Las condiciones de acceso definidas en BrowseAllow y BrowseDeny se refieren a todos los paquetes enviados a cupsd. La configuración por defecto en `/etc/cups/cupsd.conf` es la siguiente:

```
BrowseAllow @LOCAL
BrowseDeny All
```

y además

```
<Location />
  Order Deny,Allow
  Deny From All
  Allow From 127.0.0.1
  Allow From 127.0.0.2
  Allow From @LOCAL
</Location>
```

De este modo, sólo los equipos de tipo `LOCAL` pueden acceder al cupsd en el servidor CUPS. Los ordenadores `LOCAL` son aquellos cuya dirección IP no pertenece a una interfaz punto a punto (una interfaz que carece de la bandera `IFF_POINTOPOINT`) y cuya dirección IP pertenece a la misma red del servidor CUPS. Los paquetes procedentes de cualquier otro ordenador se rechazan inmediatamente.

Activación automática de cupsd

Después de una instalación estándar, `cupsd` se activa automáticamente permitiendo así acceder de forma directa a las colas de impresión de servidores CUPS

en la red sin necesidad de ninguna intervención adicional. Las dos restricciones de seguridad mencionadas (ver sección cupsd se ejecuta como usuario lp en esta página y sección Funcionalidad general de BrowseAllow y BrowseDeny en esta página) son condiciones necesarias para la activación automática de `cupsd` sin comprometer la seguridad.

12.7.4. Archivos PPD en diversos paquetes

Configuración de impresora sólo con archivos PPD

La configuración de impresora de YaST crea las colas de CUPS sólo a partir de los archivos PPD almacenados en el sistema en `/usr/share/cups/model/`. YaST compara el nombre de la impresora detectada con los nombres de fabricantes y modelos que se encuentran en los archivos PPD de `/usr/share/cups/model/`. A partir de esta información, YaST crea una base de datos con los nombres de fabricantes y modelos. De esta forma es posible seleccionar el modelo de impresora y utilizar el archivo PPD correcto.

La ventaja de la configuración exclusivamente a base de archivos PPD radica en la posibilidad de modificar los archivos PPD de `/usr/share/cups/model/`. YaST reconoce los cambios y vuelve a crear la base de datos de modelos y fabricantes. En caso de uso exclusivo de impresoras PostScript, no se requieren los archivos PPD del paquete `cups-drivers` ni los archivos PPD Gimp-Print del paquete `cups-drivers-stp`. Puede copiar los archivos PPD correspondientes a las impresoras PostScript utilizadas en `/usr/share/cups/model/` y configurar las impresoras de forma óptima. Esto no es necesario si los archivos PPD ya se encuentran en el paquete `manufacturer-PPDs`.

Archivos PPD CUPS en el paquete cups

Los siguientes archivos PPD Foomatic han sido adaptados para dar soporte especial a las impresoras PostScript de nivel 1 y 2 y se han añadido a los archivos PPD genéricos del paquete `cups`.

- `/usr/share/cups/model/Postscript-level1.ppd.gz`
- `/usr/share/cups/model/Postscript-level2.ppd.gz`

Archivos PPD en el paquete cups-drivers

Para dar soporte a las impresoras que no son PostScript se utiliza normalmente el filtro de impresión `foomatic-rip` junto con GhostScript. Los archivos PPD Foomatic adecuados se identifican con las líneas `*NickName: ... Foomatic/Ghostscript driver` y `*cupsFilter: ... foomatic-rip`. Estos archivos se encuentran en el paquete `cups-drivers`.

YaST da preferencia a un archivo PPD Foomatic cuando existe un archivo PPD Foomatic recomendado para el modelo de impresora que se reconoce por `*NickName: ... Foomatic ... (recommended)` y el paquete `manufacturer-PPDs` no contiene ningún archivo PPD más adecuado (ver abajo).

Archivos PPD Gimp-Print en el paquete cups-drivers-stp

Muchas impresoras que no son PostScript pueden utilizar el filtro `rastertoprinter` de Gimp-Print en lugar de `foomatic-rip`. Este filtro y los archivos PPD correspondientes se encuentran en el paquete `cups-drivers-stp`. Los archivos PPD Gimp-Print se encuentran en `/usr/share/cups/model/stp/` y se identifican con la líneas `*NickName: ... CUPS+Gimp-Print` y `*cupsFilter: ... rastertoprinter`.

Archivos PPD de fabricantes de impresoras en el paquete manufacturer-PPDs

El paquete `manufacturer-PPDs` contiene archivos PPD publicados con una licencia de carácter abierto. El archivo PPD del fabricante permite el uso de todas las características de la impresora PostScript y es recomendable usarlo. YaST da preferencia a un archivo PPD del paquete `manufacturer-PPDs` si se cumplen las siguientes condiciones:

- El fabricante y modelo detectado coincide con el fabricante y modelo de un archivo PPD del paquete `manufacturer-PPDs`.
- El archivo PPD de `manufacturer-PPDs` es el único adecuado para el modelo de impresora o hay otro archivo PPD de tipo Foomatic con la siguiente entrada: `*NickName: ... Foomatic/Postscript (recommended)` también para ese modelo de impresora.

De manera correspondiente, YaST no utiliza un archivo PPD de `manufacturer-PPDs` en los siguientes casos:

- El archivo PPD de `manufacturer-PPDs` no se corresponde con el nombre de fabricante y modelo. Esto pasa, por ejemplo, cuando el paquete `manufacturer-PPDs` sólo contiene un archivo PPD para modelos parecidos. Por ejemplo, un nombre como `Funprinter 1000 series` en el archivo PPD identifica toda una serie de impresoras en lugar de almacenar un archivo PPD para cada modelo.
- El archivo PPD de PostScript Foomatic no aparece como "recommended": la impresora no funciona de forma suficientemente fiable en modo PostScript (ej. por falta de memoria o de potencia de procesador) o bien no soporta PostScript de forma nativa (ej. porque el soporte nativo PostScript se realiza con un módulo opcional).

Si `manufacturer-PPDs` contiene un archivo PPD adecuado para una impresora PostScript pero YaST no lo puede configurar por las razones mencionadas, el modelo de impresora debe seleccionarse manualmente.

12.8. Posibles problemas y soluciones

En los siguientes párrafos se describen los problemas de hardware y software más frecuentes durante la impresión así como diversos métodos para solucionar o evitar estos problemas.

12.8.1. Impresora sin soporte de lenguaje estándar

Las *impresoras GDI* son aquellas que se manejan con secuencias de control especiales y sólo funcionan con los sistemas operativos para los que existe un controlador del fabricante. *GDI* es una interfaz de programación para dispositivos gráficos desarrollada por Microsoft. El problema no es la interfaz de programación, sino la restricción del acceso a la impresora a través del lenguaje propietario de la impresión.

Algunas impresoras pueden operar tanto en modo GDI como en uno de los lenguaje de impresión estándar. Para algunas impresoras GDI existen controladores propietarios del fabricante. Los inconvenientes de los controladores de impresora propietarios es que no se puede garantizar el funcionamiento con el sistema de impresión actualmente instalado ni el funcionamiento correcto de las distintas

plataformas de hardware. Las impresoras que entienden un lenguaje de impresión estándar no dependen de una versión específica del sistema de impresión ni de una plataforma de hardware determinada.

Normalmente resulta más económico comprar directamente una impresora soportada en lugar de gastar tiempo en la adaptación de un controlador de Linux propietario. Con una impresora correcta, el problema de controladores se resuelve para siempre. Nunca más hará falta instalar y configurar controladores especiales o conseguir actualizaciones de controladores cuando avance el desarrollo del sistema de impresión.

12.8.2. No existe ningún archivo PPD adecuado para una impresora PostScript

Si no existe ningún archivo PPD adecuado para una impresora PostScript dentro del paquete `manufacturer-PPDs`, debería ser posible utilizar el archivo PPD del CD de controladores del fabricante de la impresora o descargar un archivo PPD adecuado de su página web.

Los archivos PPD que aparecen como archivo (.zip) o como archivo zip autodescomprimible (`.exe`) pueden ser desempaquetados con `unzip`. Aclare primero los términos de licencia del archivo PPD y compruebe a continuación con el programa `cupstestppd` si el archivo PPD cumple la especificación "Adobe PostScript Printer Description File Format Specification, version 4.3.". El resultado "FAIL" indica fallos importantes que pueden ocasionar graves problemas. Los errores indicados por `cupstestppd` han de resolverse. Si es necesario, solicite directamente al fabricante de la impresora un archivo PPD adecuado.

12.8.3. Puertos paralelos

El método más seguro para que la impresora funcione consiste en conectarla directamente al primer puerto paralelo con la siguiente configuración en la BIOS:

- Dirección E/S (I/O address): `378` (hexadecimal)
- Interrupción: irrelevante
- Modo: `Normal`, `SPP` u `Output-Only`
- DMA: no se utiliza

Si no es posible acceder a la impresora a través del primer puerto paralelo con esta configuración, se debe indicar explícitamente la dirección de entrada y salida conforme a la configuración de la BIOS de la forma `0x378` en el archivo `/etc/modprobe.conf`. Si hay dos puertos paralelos con direcciones de entrada y salida `378` y `278`, la entrada tiene que ser `0x378,0x278`.

Si la interrupción `7` todavía está libre, se puede activar la operación en modo interrupt con una entrada en el ejemplo **??** en esta página. Antes de activarlo, hay que comprobar en `/proc/interrupts` las interrupciones utilizadas actualmente. Estas varían en función del hardware empleado en ese momento. La interrupción para el puerto paralelo tiene que estar libre. En caso de duda, utilice el modo polling con `irq=none`.

Ejemplo 12.1: */etc/modprobe.conf: interrupciones para el primer puerto paralelo*

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

12.8.4. Imprimir a través de la red

Comprobar la red Conecte la impresora directamente al ordenador y configúrela para efectuar una prueba como impresora local. Si la impresión funciona, los problemas tienen su origen en la red.

Comprobar red TCP/IP La red TCP/IP y la resolución de nombres tienen que funcionar correctamente.

Comprobar un comando `lpd` remoto El siguiente comando sirve para comprobar si realmente existe una conexión TCP a `lpd` (puerto `515`) en el ordenador ⟨*host*⟩:

```
netcat -z <host> 515 && echo ok || echo failed
```

Si no se puede acceder a `lpd`, puede ser que `lpd` no se esté ejecutando o que haya problemas generales de red.

Si `lpd` se está ejecutando correctamente en el servidor, el usuario `root` puede utilizar el siguiente comando para conseguir un informe de estado de la cola ⟨*queue*⟩ en el ordenador remoto ⟨*host*⟩.

```
echo -e "\004queue" \
  | netcat -w 2 -p 722 host 515
```

Si no hay respuesta de `lpd` significa que lpd no se está ejecutando o que hay problemas generales de red. Una respuesta de `lpd` debería aclarar por qué no es posible imprimir en la cola `queue` del ordenador `host`. Si recibe una respuesta como la del ejemplo **??** en esta página, significa que el problema se encuentra en el `lpd` remoto.

Ejemplo 12.2: *Mensaje de error de lpd*

```
lpd: your host does not have line printer access
lpd: queue does not exist
printer: spooling disabled
printer: printing disabled
```

Comprobar un comando `cupsd` remoto

El siguiente comando sirve para detectar la existencia de un servidor CUPS en la red, ya que este anuncia su disponibilidad cada 30 segundos mediante un broadcast en el puerto UDP `631`:

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

Si en la red existe un servidor CUPS emitiendo broadcasts, la salida del comando será parecida a la del ejemplo **??** en esta página:

Ejemplo 12.3: *Broadcast del servidor CUPS*

```
ipp://host.domain:631/printers/queue
```

El siguiente comando comprueba la existencia de una conexión TCP a `cupsd` (puerto `631`) en el ordenador ⟨*host*⟩:

```
netcat -z host 631 && echo ok || echo failed
```

Si no hay conexión a `cupsd`, significa que `cupsd` no se está ejecutando o que hay problemas generales de red. Si `cupsd` se está ejecutando correctamente en el servidor, el comando `lpstat -h host -l -t` genera un informe (posiblemente muy extenso) de estado de todas las colas en el ordenador remoto ⟨*host*⟩.

Con el siguiente comando se comprueba si la cola ⟨*queue*⟩ del ordenador ⟨*host*⟩ acepta una tarea de impresión compuesta por un único retorno de carro; es decir, no se deberá imprimir nada o, como máximo, una hoja en blanco.

```
echo -en "\r" \
  | lp -d queue -h host
```

Búsqueda de errores en una impresora de red o servidor de impresión

En ocasiones hay problemas con el spooler de impresión de un servidor de impresión (printserver-box), sobre todo cuando tienen que manejar un gran número de tareas de impresión. Dado que el problema radica en el spooler del servidor, no hay solución directa. La solución indirecta consiste en evitar el spooler accediendo directamente a la impresora a través de socket TCP. Consulte a este respecto la sección **??** en esta página.

De este modo el servidor de impresión sólo trabaja como conversor entre los diferentes formatos de datos (red TCP/IP y conexión local). Para realizar el desvío hace falta conocer el puerto TCP correspondiente en el servidor de impresión. Con impresora y servidor de impresión encendidos, se puede utilizar para ello el programa `nmap` del paquete `nmap`. Por ejemplo, el comando `nmap` ⟨*`dirección-IP`*⟩ devuelve el siguiente resultado para un servidor de impresión:

```
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 de nmap significa que se puede acceder al servidor a través del puerto `9100`. En su configuración predeterminada, `nmap` sólo comprueba una lista de puertos conocidos que se incluye en en `/usr/share/nmap/nmap-services`. Para comprobar todos los puertos posibles, utilice el comando: `nmap -p` ⟨*`from_port`*⟩`-`⟨*`to_port`*⟩ ⟨*`dirección-IP`*⟩. Esta operación puede llevar bastante tiempo; véase también la página man de `nmap`.

Introduzca un comando como:

```
echo -en "\rHolaMundo\r\f" | netcat -w 1 IP-address port
cat file | netcat -w 1 IP-address port
```

para enviar directamente cadenas de caracteres o archivos a un puerto determinado para comprobar si es posible acceder a la impresora a través de ese puerto. En caso afirmativo, se imprimirán las palabras ”HolaMundo”.

12.8.5. Impresión defectuosa sin que se hayan producido mensajes de error

El sistema de impresión da por terminada la tarea de impresión cuando CUPS finaliza la transferencia de datos a la impresora. Si la impresión posteriormente fracasa (por ejemplo porque la impresora no interpreta los datos de impresión correctamente), el sistema de impresión no se da cuenta de ello. En caso de que la impresora no sea capaz de imprimir los datos correctamente, deberá buscarse un archivo PPD más adecuado.

12.8.6. Colas de impresión desactivadas

Después de varios intentos fallidos de enviar los datos a la impresora, el dorsal de CUPS (por ejemplo `usb` o `socket`) notifica un error al sistema de impresión (concretamente a `cupsd`). El dorsal determina a partir de cuántos intentos se notifica un error. Dado que no tiene sentido realizar intentos adicionales, `cupsd` desactiva (`disable`) la cola en cuestión. Después de solucionar el problema, el administrador del sistema tiene que reactivar la cola mediante el comando `/usr/bin/enable`.

12.8.7. Borrar tareas de impresión cuando CUPS practica browsing

Un servidor de red CUPS que ofrece sus colas por medio de browsing, recibe las tareas de impresión desde los `cupsd` que se ejecutan localmente en los ordenadores cliente. Estos `cupsd` locales se encargan de recibir las tareas de impresión de las aplicaciones y pasarlas al `cupsd` del servidor. Cada vez que `cupsd` recibe una tarea de impresión le asigna un número, por lo que el número de tarea en cliente y en el servidor no es el mismo. Puesto que la tarea de impresión se reenvía inmediatamente y el `cupsd` del cliente da por concluida su función cuando envía dicha tarea al `cupsd` del servidor, no es posible borrar en el servidor una tarea de impresión con el número del cliente.

Para borrar la tarea en el servidor es preciso averiguar su número en el servidor por medio de un comando como `lpstat -h print-server -o`. Para ello es preciso que el servidor no haya completado la tarea de impresión (es decir, que todavía no la haya enviado a la impresora). Una vez que se conoce el número, es posible borrar la tarea de impresión con:

```
cancel -h print-server cola-número_tarea
```

12.8.8. Error de tarea de impresión o de transferencia de datos

Las tareas de impresión se mantienen en las colas y puede que se vuelvan a imprimir desde el principio tras apagar y encender la impresora o reiniciar el ordenador durante la impresión. Para eliminar permanentemente una tarea de impresión de la cola, utilice el comando `cancel`.

En caso de una tarea de impresión defectuosa o de interferencias en la transferencia de datos, la impresora no sabe interpretar los datos correctamente y el resultado es un gran número de hojas impresas llenas de caracteres sin sentido. Si esto sucede, realice los siguientes pasos:

1. Retire el papel de las impresoras de chorro de tinta o abra la bandeja de papel en las impresoras láser para detener la impresión. Las impresoras de calidad disponen de un botón para detener la tarea de impresión en curso.
2. Debido a que la tarea de impresión permanece en la cola hasta su envío completo a la impresora, normalmente todavía se encontrará allí tras apagar ésta. Utilice el comando `lpstat -o` o `lpstat -h` ⟨*print-server*⟩ `-o` para comprobar cuál es la cola de impresión actualmente activa y borre la tarea con `cancel` ⟨*cola*⟩`-`⟨*número_tarea* ⟩ o con `cancel -h` ⟨*print-server*⟩ ⟨*cola*⟩`-`⟨*número_tarea*⟩ .
3. En caso de que se sigan transmitiendo datos a la impresora a pesar de haber borrado la tarea de la cola, compruebe si se está ejecutando un proceso dorsal de CUPS para la cola en cuestión y termínelo en caso afirmativo. El comando `fuser -k /dev/lp0` termina por ejemplo todos los procesos que aún estén accediendo a la impresora en el puerto paralelo.
4. Desconecte la impresora completamente desenchufándola unos minutos. Posteriormente vuelva a introducir papel y encienda la impresora.

12.8.9. Depuración del sistema de impresión CUPS

Se recomienda el siguiente procedimiento para localizar problemas en el sistema de impresión CUPS:

1. Active el nivel de registro `LogLevel debug` en `/etc/cups/cupsd.conf`.

2. Detenga `cupsd`.
3. Elimine `/var/log/cups/error_log*` para no tener que buscar en archivos demasiado grandes.
4. Inicie `cupsd`.
5. Repita la operación que ha causado el error.
6. Examine los mensajes disponibles en `/var/log/cups/error_log*` para averiguar la causa del problema.

12.8.10. Información adicional

En nuestra base de datos de soporte (SDB) se incluyen las soluciones a muchos problemas específicos. En caso de dificultades con impresoras, consulte los artículos *Installing a Printer* y *Printer Configuration from SUSE LINUX 9.2* a los que puede acceder introduciendo el término de búsqueda "printer".

Movilidad con Linux

En este capítulo se describen las diferentes cuestiones relacionadas con la movilidad al trabajar con Linux. En él se describen brevemente los diferentes campos de aplicación y las correspondientes soluciones tanto a nivel de software como de hardware. Finalmente, se adjunta una lista de las principales fuentes de información a las que puede acceder relacionadas con este tema.

La mayoría de los usuarios asocia el trabajo móvil con portátiles, PDAs y teléfonos móviles y con sus posibilidades de comunicación. Este capítulo amplía este concepto al tratar elementos móviles de hardware tales como discos duros externos, memorias extraíbles USB o cámaras digitales que pueden interactuar con portátiles o sistemas de sobremesa.

13.1. Trabajo móvil con portátiles

13.1.1. Particularidades del hardware de los portátiles

El equipamiento que ofrecen los portátiles se distingue del de los ordenadores de sobremesa en base a criterios como la transportabilidad, el consumo de energía y los requerimientos de espacio, elementos decisivos a la hora del trabajo móvil. Para solucionar algunas de estas cuestiones, los fabricantes de hardware desarrollaron el estándar PCMCIA (*Personal Computer Memory Card Internacional Association*). Este estándar contempla tarjetas de memoria, tarjetas de red, tarjetas para conexión ADSL, tarjetas módem y discos duros externos. En el capítulo **??** en esta página puede encontrar una descripción detallada acerca del soporte que ofrece Linux para este tipo de hardware así como información relativa a cuestiones tales como qué es necesario tener en cuenta durante la configuración, la disponibilidad de herramientas para vigilar el funcionamiento de los conectores PCMCIA y cómo solucionar los posibles problemas en caso de que se muestren mensajes de error.

13.1.2. Ahorro de energía

En la fabricación de equipos portátiles, uno de los factores clave consiste en realizar un diseño basado en pocos componentes y optimizar estos para que su consumo sea lo más bajo posible a fin de aumentar la autonomía del sistema. La contribución al ahorro de energía de su sistema operativo es, como mínimo, igual de importante. SUSE LINUX soporta distintos métodos para gestionar el consumo de energía del portátil y que ofrecen diferentes resultados en relación a la duración de la batería. Hemos ordenados estos según su efectividad a la hora de prolongar la autonomía del portátil:

- Reducción de la frecuencia del procesador.
- Apagado de la iluminación de la pantalla durante periodos de inactividad.

- Reducción manual de la iluminación de la pantalla.
- Desconexión de periféricos extraíbles en caliente que no estén siendo utilizados (CDROM USB, ratón externo, tarjetas PCMCIA, etc.).
- Desconexión del disco duro si no está siendo utilizado.

Puede obtener información adicional acerca de la gestión de energía en SUSE LINUX y el manejo del módulo de gestión de energía de YaST en el capítulo **??** en esta página.

13.1.3. Integración en entornos operativos dinámicos

Durante el trabajo móvil, es frecuente que los sistemas deban integrarse en diferentes entornos. Existen muchas funcionalidades que son dependientes de éstos y, normalmente, los servicios básicos han de ser configurados de nuevo. SUSE LINUX se hace cargo de esta tarea.

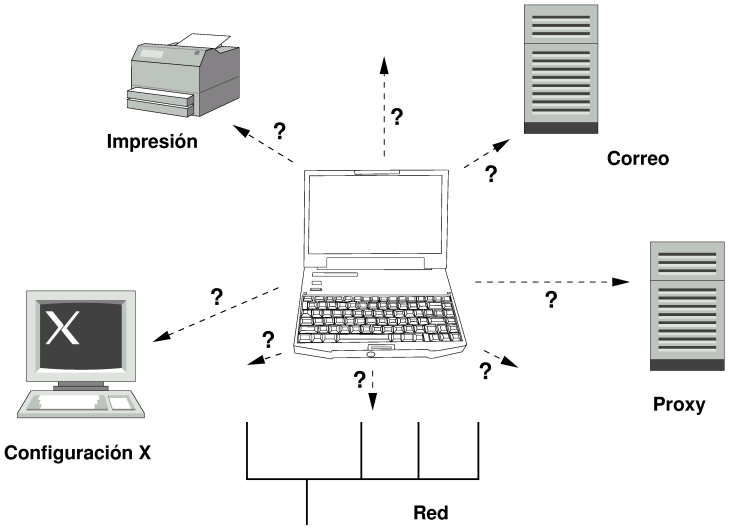

Figura 13.1: *Integración de un portátil en la red*

En el caso de un equipo portátil que se emplee alternativamente en una pequeña red doméstica y una corporativa, las funcionalidades y servicios afectados son:

Configuración de la red Este aspecto comprende la asignación de direcciones IP, la resolución de nombres y la conexión a Internet o a otras redes.

Impresión Debe existir una base de datos actualizada conteniendo las impresoras operativas y, dependiendo de la red, también es necesario poder acceder a un servidor de impresión.

Correo electrónico y proxies Como en el caso de la impresión, la lista de los servidores correspondientes ha de estar actualizada.

Configuración X En caso de que conecte temporalmente el portátil a un proyector o un monitor externo, la configuración de pantalla ha de conservarse igualmente.

Con SUSE LINUX dispone de dos posibilidades que pueden combinarse para integrar su portátil en entornos operativos existentes:

SCPM SCPM (*System Configuration Profile Management*) le permite guardar cualquier estado de configuración de sistema (denominado *perfil*) de manera ”instantánea”. Pueden crearse perfiles para las más diversas situaciones. Estos se ofrecen cada vez que el sistema se conecta a un entorno distinto (redes domésticas/redes corporativas). Asimismo, puede emplear esta opción para disponer de una configuración de trabajo y otra para experimentar nuevas aplicaciones, etc. Es posible en todo momento acceder al resto de perfiles. Puede encontrar más información acerca de SCPM en el capítulo ?? en esta página. En KDE, puede cambiar de perfil mediante la funcionalidad Profile Chooser. Naturalmente, por cuestiones de seguridad, el sistema le solicitará la contraseña de root antes de poder realizar ningún cambio.

SLP El *Service Location Protocol* (abreviado: SLP) simplifica la configuración de clientes integrados dentro de una red local. Para configurar su portátil en un entorno de red, necesitaría tener un cierto grado de conocimientos a nivel de administrador acerca del servidor de la red. Con SLP, se da a conocer a todos los clientes la disponibilidad de un determinado tipo de servicio en la red local. Las aplicaciones que soportan SLP pueden utilizar la información distribuida mediante este protocolo, por lo que pueden configurarse automáticamente. SPL puede utilizarse incluso para la instalación de un sistema sin necesidad de que sea preciso buscar una fuente de instalación adecuada. Puede encontrar más información acerca de SLP en la capítulo ?? en esta página.

Lo esencial de SCPM es que permitir y obtener condiciones del sistema reproducibles, mientras que SLP facilita enormemente la configuración automática de un ordenador conectado a red.

13.1.4. Software

Existen diferentes aspectos sensibles que pueden ser resueltos mediante software específico durante el trabajo móvil: vigilancia del sistema (sobre todo, la carga de la batería), sincronización de datos y comunicación inalámbrica con equipos periféricos e Internet. Los siguientes apartados describen para cada punto las aplicaciones más importantes contenidas en SUSE LINUX.

Vigilancia del sistema

Este apartado describe dos herramientas de KDE para la vigilancia del sistema contenidas en SUSE LINUX. La aplicación KPowersave de Kicker gestiona el indicador de estado de la batería del portátil. Por otro lado, KSysguard se encarga de la monitorización del sistema más compleja. En GNOME, las funciones descritas residen en GNOME ACPI (como aplicación de panel) y System Monitor.

KPowersave KPowersave es un applet que proporciona información básica a través de un pequeño icono ubicado en la barra de herramientas acerca del nivel de carga de la batería. El icono se adapta según el tipo de suministro de energía. En caso de alimentación por red, verá un pequeño icono con forma de enchufe; en caso de alimentación por batería, se muestra un icono en forma de batería. Después de introducir la contraseña de root, inicie el módulo YaST para la gestión de energía a través del menú correspondiente. Desde él, puede establecer varias opciones de configuración según las diferentes fuentes de energía. Puede obtener más información acerca de la administración de energía y el módulo YaST correspondiente en el capítulo ?? en esta página.

KSysguard KSysguard es una aplicación que aglutina todos lo parámetros que pueden ser controlados dentro del sistema. KSysguard posee controladores para ACPI (nivel de la batería), la tasa de utilización del procesador, la red, la ocupación de las particiones, la carga del procesador y la utilización de memoria. Además, puede producir una lista de todos los procesos del sistema. Sólo ha de establecer el tipo de presentación o filtrado. Es capaz de controlar diferentes parámetros del sistema o incluso recopilar de forma simultánea los datos de diferentes ordenadores a través de la red. KSysguard

puede utilizarse también como daemon en ordenadores que no dispongan de ningún entorno KDE. Puede obtener más información acerca de este programa mediante su función de ayuda o a través de la ayuda de SUSE.

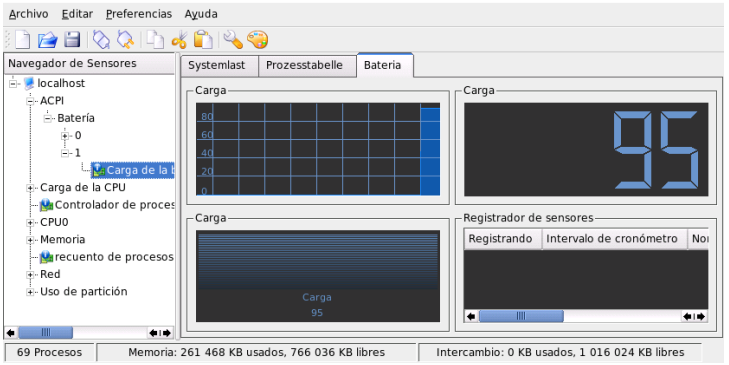

Figura 13.2: *Control del nivel de la batería con KSysguard*

Sincronización de datos

Si alterna el trabajo móvil sin conexión a la red mediante el portátil con el empleo de un sistema conectado a la red en la empresa, se encontrará ante el problema de mantener sincronizados todos los datos almacenados en ambos ordenadores, tales como carpetas de correo electrónico o documentos de texto. Puede encontrar soluciones a tales cuestiones en los siguientes apartados:

Sincronización del correo electrónico

Utilice en la red corporativa una cuenta IMAP para almacenar sus mensajes electrónicos. Lea sus correos en la estación de trabajo con cualquier programa de correo que soporte IMAP (Mozilla Thunderbird Mail, Evolution o KMail, véase *Manual de usuario*). Configure el programa de correo en todos los equipos desde los que lea el correo, de manera que se utilice siempre la misma carpeta para los `mensajes enviados`. De esta manera, podrá acceder siempre a todos los mensajes y dispondrá de los marcadores de estado correcto tras el proceso de sincronización. Utilice en todos los casos el servicio SMTP para el envío de correo, soportado en todos los clientes de correo, en lugar de MTA (postfix o sendmail).

Sincronización de documentos/archivos individuales
Existen varias utilidades que resultan apropiadas para la sincronización de datos entre portátiles y ordenadores de sobremesa. Si desea obtener más información al respecto, consulte el capítulo **??** en esta página.

Comunicación inalámbrica

Además de poder conectarse a una red doméstica o corporativa basada en cables, muchos portátiles pueden comunicarse sin cables con otros ordenadores, dispositivos, teléfonos móviles o PDAs. Linux soporta tres tipos de comunicación inalámbrica:

WLAN Gracias a su mayor alcance, WLAN es, entre las tecnologías denominadas inalámbricas, la única apta para el despliegue de redes amplias y separadas geográficamente. De esta forma, es posible conectar, por ejemplo, un ordenador mediante WLAN a una red inalámbrica o a Internet. Los puntos de acceso conforman una especie de estación base que proporciona acceso al resto de la red. El usuario móvil puede conectarse a distintos puntos de acceso dependiendo de dónde se encuentre en cada momento y de qué punto de acceso proporciona la mejor conexión. Como en la telefonía móvil, el usuario WLAN dispone de una gran red que no le restringe espacialmente. Puede obtener más detalles acerca de las redes WLAN en el sección **??** en esta página.

Bluetooth Bluetooth es una de las tecnologías inalámbricas más empleada. Al igual que IrDA, puede utilizarse para la comunicación entre un ordenador (normalmente un portátil) y un PDA o teléfono móvil. También puede emplearse para conectar diferentes ordenadores entre sí, siempre que se disponga de una línea de visión directa entre ellos. Además, Bluetooth puede emplearse para integrar periféricos inalámbricos como teclados o ratones. No obstante, el alcance de esta tecnología no es suficiente como para enlazar sistemas ubicados en diferentes lugares. Para comunicarse de manera inalámbrica a través de obstáculos espaciales tales como paredes, es necesario emplear WLAN. Puede encontrar más información acerca de Bluetooth, de sus posibilidades de utilización y de su configuración en la sección **??** en esta página.

IrDA IrDA es la tecnología inalámbrica que ofrece el menor rango de alcance. Los dos interlocutores tienen que colocarse uno frente al otro. Los obstáculos, como paredes de habitaciones, no pueden superarse. El escenario más típico para la utilización de IrDA es el envío de un archivo desde un portátil

a un teléfono móvil. El pequeño trayecto entre el portátil y el teléfono móvil puede recorrerse a través de IrDA. Otra posibilidad de utilización de IrDA es el envío inalámbrico de órdenes a una impresora. Puede obtener más información acerca de IrDA en la sección **??** en esta página.

13.1.5. Seguridad de datos

Es recomendable que proteja de la mejor forma posible los datos de su portátil contra accesos no autorizados. Las medidas de seguridad que puede tomar pueden clasificarse según los siguientes aspectos:

Protección contra robo Si es posible, proteja siempre su sistema contra robos. Existen varios sistemas de seguridad en el mercado (por ejemplo, dispositivos de sujección a la mesa).

Protección de datos en el sistema Codifique los datos importantes no sólo durante su transmisión a través de una red, sino también en el disco duro. De esta manera, sus datos no se verán comprometidos en caso de robo. Puede obtener más información acerca de cómo crear una partición codificada bajo SUSE LINUX en la sección **??** en esta página.

Seguridad en red La transferencia de datos desde y hacia su interlocutor debería estar siempre protegida, sin importar cómo se lleve a cabo físicamente la comunicación. Puede obtener información detallada acerca de los aspectos generales de seguridad bajo Linux y redes en la sección **??** en esta página. También puede encontrar documentación adicional acerca de los aspectos de seguridad en redes inalámbricas en el capítulo sobre comunicación inalámbrica capítulo ?? en esta página.

13.2. Hardware móvil

SUSE LINUX soporta la conexión automática de dispositivos extraíbles de memoria a través de Firewire (IEEE 1394) o USB. El término dispositivos extraíbles de memoria comprende todo tipo de discos duros Firewire/USB, memorias extraíbles tipo USB o cámaras digitales. Una vez que se conectan estos dispositivos a través de la interfaz correspondiente, son reconocidos y configurados automáticamente por el sistema. subfs/submount se ocupa de montar los dispositivos en el

lugar correspondiente en el sistema de archivos. De esta forma, se ahorra el tener que montar y desmontar manualmente los dispositivos. Si ningún programa está accediendo a alguno de estos periféricos, puede simplemente desconectarlo.

Discos duros externos (USB y Firewire)
Una vez que el sistema detecta correctamente un disco duro externo, puede ver el correspondiente icono en 'Mi ordenador' (KDE) o en 'Computer' (GNOME) en la lista de unidades conectadas. Pulse el botón izquierdo del ratón sobre el icono y se le mostrará el contenido de la unidad. Puede crear, editar o borrar archivos y carpetas. Si desea cambiar el nombre asignado por el sistema por otro, pulse el botón derecho sobre el icono para activar el correspondiente menú desplegable y modifique el nombre. No obstante, recuerde que este cambio de nombre está limitado sólo al mostrado en el administrador de archivos — el nombre con el que está montado el dispositivo en `/media/usb-xxx` o `/media/ieee1394-xxx` permanece intacto.

Memorias extraíbles USB El sistema trata a las memorias USB de la misma manera que a los discos duros externos. También se puede cambiar su nombre en el administrador archivos.

Cámaras digitales (USB y Firewire) Las cámaras digitales reconocidas por el sistema aparecen igualmente como unidades externas en la lista del administrador de archivos. En KDE puede seleccionar y visualizar las fotos a través de la URL `camera:/`. Utilice digikam o The GIMP para editar las fotos. En GNOME, puede visualizar las fotos en Nautilus desde la carpeta correspondiente. GThumb se encarga de la gestión y edición básica de las fotos. Si necesita realizar cambios más complejos, utilice The GIMP. Todos los programas mencionados se encuentran descritos en el *Manual de usuario*, a excepción de GThumb. Asimismo, puede consultar el capítulo dedicado a las cámaras digitales.

Importante

Protección de soportes móviles

Al igual que los portátiles, los discos duros móviles o las memorias extraíbles son susceptibles de ser robados. Para evitar que se haga un uso indebido y no autorizado de los datos contenidos por parte de terceros, se recomienda crear una partición cifrada como se describe en la sección **??** en esta página.

Importante

13.3. Comunicación móvil: teléfonos móviles y PDAs

La comunicación entre un sistema de sobremesa o un portátil y un teléfono móvil puede llevarse a cabo a través de Bluetooth o IrDA. Algunos modelos soportan ambos protocolos, otros sólo uno de los dos. Ya se han comentado los ámbitos de utilización de ambos protocolos y su correspondiente documentación adicional en la sección Comunicación inalámbrica en esta página. En la documentación de los dispositivos se describe cómo se autoconfiguran estos protocolos en el teléfono móvil. La descripción de la configuración bajo Linux está disponible en la sección **??** en esta página y sección **??** en esta página.

El soporte de sincronización con dispositivos Palm está integrado en Evolution y Kontact. La primera conexión con el Palm puede llevarse a cabo fácilmente en ambos casos con la ayuda de un asistente. Una vez que se haya configurado, determine qué tipo de datos desea sincronizar (contactos, citas, etc.). Ambos programas están descritos en el *Manual de usuario*.

El programa KPilot integrado en Kontact está disponible también como programa independiente; puede encontrar una descripción en el *Manual de usuario*. Además, dispone del programa KitchenSync para la sincronización de direcciones.

Si desea obtener información adicional acerca de Evolution y Kontact, puede encontrarla en el *Manual de usuario*.

13.4. Información adicional

Uno de los mejores sitios de soporte relacionado con dispositivos móviles bajo Linux es `http://tuxmobil.org/`. Varias secciones de este sitio web tratan aspectos de hardware y software relacionados con portátiles, PDAs, teléfonos móviles y otro hardware móvil.

Puede encontrar un sitio web de temática similar a la de `http://tuxmobil.org/` en `http://www.linux-on-laptops.com/`. Aquí podrá acceder a abundante información acerca de portátiles y dispositivos de mano:

SUSE mantiene una lista de correo propia sobre temas relacionados con portátiles (en alemán): `http://lists.suse.com/archive/suse-laptop/`. Usuarios y fabricantes debaten en esta lista todos los aspectos relacionados con el trabajo

móvil bajo SUSE LINUX. Las consultas expuestas en inglés suelen ser contestadas; no obstante, recuerde que la mayor parte de la información archivada está disponible únicamente en alemán.

En caso de problemas relacionados con la administración de energía en portátiles bajo SUSE LINUX, le recomendamos que consulte los archivos `README` ubicados en `/usr/share/doc/packages/powersave`. Estos archivos contienen la información más reciente acerca de los últimos comentarios, sugerencias o avances respecto al trabajo de los desarrolladores, por lo que es muy frecuente encontrar valiosos consejos encaminados a la resolución de problemas.

PCMCIA

Este capítulo describe las peculiaridades del hardware de portátiles y más concretamente de PCMCIA desde el punto de vista del hardware y software. PCMCIA es la abreviatura de *Personal Computer Memory Card International Association* y se usa por extensión para denominar todo el hardware y software relacionado.

14.1. Hardware

El componente clave es la tarjeta PCMCIA, de la que se distinguen dos tipos:

Tarjetas PC Estas tarjetas existen desde los orígenes de PCMCIA. Utilizan un bus de 16 bits para la transferencia de datos y suelen ser bastante económicas. Algunos puentes PCMCIA modernos tienen dificultades para detectar estas tarjetas. No obstante, una vez detectadas son estables y no ocasionan problemas.

Tarjetas CardBus Estas tarjetas constituyen un estándar más nuevo. Utilizan un bus de 32 bits de anchura, por lo que son más rápidas pero también más caras. Se integran en el sistema como las tarjetas PCI y su uso no presenta ningún problema.

Cuando el servicio PCMCIA está activo, el comando `cardctl ident` indica qué tarjeta está introducida en la ranura. Una lista de las tarjetas soportadas se encuentra en `SUPPORTED.CARDS` en el directorio `/usr/share/doc/packages/pcmcia`. Allí se recoge también la versión más actual 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. Se soportan todos los modelos de uso extendido. Con el comando `pcic_probe` se puede averiguar el tipo de controladora. Si se trata un dispositivo PCI, puede obtener información adicional con el comando `lspci -vt`.

14.2. Software

A continuación se explica PCMCIA desde el punto de vista del software tratando, por un lado, los módulos del kernel envueltos en el proceso y, por otro, el administrador de tarjetas.

14.2.1. Los módulos base

Los módulos del kernel necesarios se encuentran en los paquetes del kernel. También se requieren los paquetes `pcmcia` y `hotplug`. Al arrancar PCMCIA se cargan los módulos `pcmcia_core`, `yenta_socket` y `ds`. En muy raras ocasiones se necesita el módulo `tcic` en lugar de `yenta_socket`. Estos módulos inician las controladoras PCMCIA disponibles y proporcionan funciones básicas.

14.2.2. El administrador de tarjetas

Para que las tarjetas PCMCIA puedan intercambiarse, debe controlarse la actividad de las ranuras de conexión. De esta función se encargan los servicios de tarjeta (*CardServices*) implementados en los módulos base. El administrador de tarjetas (*Cardmanager*) y el sistema hotplug del kernel se encargan de iniciar las tarjetas PC y CardBus respectivamente. El administrador de tarjetas es activado por el script de inicio de PCMCIA tras cargar los módulos base. Hotplug se activa automáticamente.

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, montar particiones de discos SCSI externos o llevar a cabo otras acciones específicas del hardware. Los scripts del administrador de tarjetas se encuentran en el directorio `/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, todas las actividades de la tarjeta. Finalmente, los módulos que ya no se necesitan se descargan de la memoria.

Para procesos de este tipo existen los llamados ”hotplug events”. Cuando se añaden discos duros o particiones (”block events”), los scripts hotplug se encargan de que los nuevos medios de almacenamiento estén disponibles inmediatamente en `/media` por medio de `subfs`. Para montar medios de almacenamiento a través de los antiguos scripts PCMCIA, `subfs` debe estar desconectado en hotplug.

Tanto los protocolos de inicio de los sistemas PCMCIA como todas las acciones de la tarjeta quedan guardados en el archivo de registro del sistema (`/var/log/messages`). Allí se recoge qué módulos se han cargado y que scripts se han utilizado 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 no exista ninguna conexión a la red. Sin embargo, esto no funciona en combinación con las particiones montadas de un disco externo o con directorios NFS. En este caso se debe garantizar que las unidades estén sincronizadas y se desmonten correctamente. Por supuesto, esto no es posible cuando la tarjeta ya se ha extraído. En caso de duda, utilice `cardctl eject`. Este comando desactiva todas las tarjetas que se encuentran en el portátil. Si quiere desactivar solamente una tarjeta, añada el número de ranura. Por ejemplo `cardctl eject 0`.

14.3. Configuración

Para especificar si se debe iniciar PCMCIA al encender el ordenador, utilice el editor de niveles de ejecución de YaST. Para iniciar este módulo seleccione 'Sistema' → 'Editor de niveles de ejecución'.

En el archivo `/etc/sysconfig/pcmcia` se definen las siguientes tres variables:

`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 concebida como parámetro para el módulo `pcmcia_core`, pero casi nunca es necesario utilizarla. Estas opciones se describen en las páginas del manual pcmcia_core(4). Puesto que estas páginas se refieren al módulo homónimo del paquete `pcmcia-cs` de David Hinds, incluyen más parámetros de los que realmente ofrece el módulo del kernel, concretamente todos los que empiezan por `cb_` y `pc_debug`.

`PCMCIA_BEEP` activa y desactiva las señales acústicas del administrador de tarjetas.

La asignación de controladores a tarjetas PC para el administrador de tarjetas se encuentra en los archivos `/etc/pcmcia/config` y `/etc/pcmcia/*.conf`. En primer lugar se lee `config` y después `*.conf` en orden alfabético. La última entrada para una tarjeta es la decisiva. Los detalles sobre la sintaxis se encuentran en la página del manual pcmcia(5).

La asignación de controladores a tarjetas CardBus se lleva a cabo en los archivos `/etc/sysconfig/hardware/hwcfg-<descripción_de_dispositivo>`. YaST crea estos archivos al configurar la tarjeta. Puede obtener información adicional sobre las descripciones de dispositivo en `/usr/share/doc/packages/sysconfig/README` y en la página del manual getcfg(8).

14.3.1. Tarjetas de red

Las tarjetas de red Ethernet, Wireless LAN y TokenRing se pueden instalar como tarjetas de red corrientes con YaST. Si la tarjeta no es detectada, basta con escoger la opción `PCMCIA` como tipo de tarjeta en la configuración del hardware. Todos los detalles adicionales sobre la configuración de red se encuentran en la sección ?? en esta página.

14.3.2. 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 tarjetas RDSI PCMCIA se escoja; lo que importa es que se trate de una tarjeta PCMCIA. Al configurar el hardware y el proveedor, compruebe que el modo de funcionamiento es `hotplug` y no `onboot`. También existen modems RDSI para tarjetas PCMCIA. Se trata de tarjetas de módem o multitarea que incorporan un kit de conexión RDSI y se comportan como un módem.

14.3.3. Módem

Las tarjetas PC de módem normalmente no conocen ninguna configuración específica para PCMCIA. Cuando se inserta un módem, este está disponible directamente en `/dev/modem`. También existen los llamados softmodems para las tarjetas PCMCIA, pero por lo general no están soportados. En caso de que exista un controlador, debe instalarse en el sistema.

14.3.4. SCSI e IDE

El administrador de tarjetas o Hotplug carga el módulo adecuado. Nada más insertar una tarjeta SCSI o IDE, los dispositivos conectados, cuyos nombres se averiguan dinámicamente, ya se encuentran disponibles. Puede obtener información adicional sobre los dispositivos SCSI e IDE disponibles en `/proc/scsi` o `/proc/ide`.

Los discos duros externos, las unidades de 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.

Aviso

Extracción de tarjetas SCSI o IDE

Antes de extraer una tarjeta SCSI o IDE es necesario desmontar todas las particiones de los dispositivos conectados (con el comando `umount`). Si olvida desmontarlos, deberá reiniciar el sistema para poder acceder de nuevo a estos dispositivos.

Aviso

14.4. Herramientas de ayuda adicionales

El programa cardctl, que ya ha sido mencionado más arriba, es la herramienta principal para conseguir información sobre PCMCIA así como para ejecutar determinadas acciones. Puede encontrar información adicional sobre el programa en la página del manual cardctl(8). También se puede introducir `cardctl` para que aparezca una lista con los comandos válidos. Para este programa también existe un frontal gráfico, cardinfo, que permite controlar las funciones principales. Para utilizarlo, el paquete `pcmcia-cardinfo` debe estar instalado.

Otras herramientas 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 utilizar el comando `rpm -ql pcmcia`.

14.5. Posibles problemas y sus soluciones

La mayoría de problemas relacionados con PCMCIA en algunos portátiles o con determinadas tarjetas puede solucionarse sin demasiado esfuerzo siempre que se proceda sistemáticamente. En primer lugar hay que averiguar si el problema se encuentra en una tarjeta o en el sistema base PCMCIA. Por este motivo, en primer lugar debe iniciarse el ordenador sin haber insertado ninguna tarjeta. La tarjeta se insertará una vez que sea obvio que el sistema base funciona correctamente. Todos los mensajes del sistema se registran en `/var/log/messages`, por lo que se recomienda observar este archivo durante las pruebas con `tail -f /var/log/messages`. De este modo el problema puede reducirse a uno de los dos casos siguientes:

14.5.1. El sistema base PCMCIA no funciona

Si el sistema se detiene durante el arranque con el mensaje PCMCIA: Starting services o si se producen otras incidencias extrañas, se debe introducir `NOPCMCIA=yes` en el prompt de arranque para desactivar el servicio PCMCIA en el próximo arranque. Para reducir aún más la causa del error, cargue los tres módulos base del sistema PCMCIA utilizado manualmente y de forma secuencial.

Ejecute como usuario `root` los comandos `modprobe pcmcia_core`, `modprobe yenta_socket` y `modprobe ds` para cargar los módulos PCMCIA manualmente. En algunos casos excepcionales se utilizará uno de los módulos `tcic`, `i82365` o `i82092` en lugar de `yenta_socket`. Los módulos críticos son los dos primeros.

La página man pcmcia_core(4) le será de utilidad si el error aparece al cargar `pcmcia_core`. Las opciones que se mencionan en dicha página se pueden probar primero con el comando `modprobe`. Por ejemplo, es posible comprobar las secciones E/S libres. Esta prueba puede ocasionar problemas en algunos casos si se interfiere con otros componentes de hardware. Esto se evita con la opción `probe_io=0`:

```
modprobe  pcmcia_core probe_io=0
```

Si la opción probada tiene éxito, se asigna el valor `probe_io=0` a la variable `PCMCIA_CORE_OPTS` en el archivo `/etc/sysconfig/pcmcia`. Cuando se utilizan múltiples opciones, se separan con espacios:

```
PCMCIA_CORE_OPTS="probe_io=0 setup_delay=10"
```

La aparición de errores al cargar el módulo `yenta_socket` es un síntoma de problemas más generales como puede ser la distribución de recursos por parte de ACPI.

El administrador de tarjetas analiza los archivos `/etc/pcmcia/config` y `/etc/pcmcia/config.opts`. Una parte de las opciones de configuración allí recogidas es relevante para el inicio de cardmgr y la otra para la carga de módulos de controladores para las tarjetas PC. En el archivo `/etc/pcmcia/config.opts` también es posible incluir o excluir IRQs, puertos E/S y secciones de memoria. En algunos casos excepcionales, el acceso a una sección E/S incorrecta provoca un fallo total del sistema. Si esto ocurre, conviene realizar pruebas aislando sucesivamente estas secciones.

14.5.2. La tarjeta PCMCIA no funciona correctamente

Fundamentalmente, hay tres razones por las que una tarjeta PCMCIA puede no funcionar correctamente: no se reconoce la tarjeta, no se puede cargar el controlador o la interfaz ofrecida por el controlador está mal configurada. Debe tenerse en cuenta si la tarjeta es gestionada por el administrador de tarjetas o por el hotplug. Como ya hemos visto, el administrador de tarjetas se ocupa de las tarjetas PC y hotplug de las tarjetas CardBus.

No se produce ninguna reacción al insertar la tarjeta
Si el sistema no reacciona cuando se introduce una tarjeta y la ejecución del comando `cardctl insert` tampoco produce ningún resultado, es un posible síntoma de que la asignación de interrupciones a dispositivos PCI es incorrecta. A veces el problema también reside en otros dispositivos PCI como las tarjetas de red. En este caso puede utilizarse el parámetro de arranque `pci=noacpi` u otros parámetros PCI o ACPI.

La tarjeta no se detecta Si no se reconoce la tarjeta, el mensaje unsupported Card in Slot x aparece en `/var/log/messages`. Este mensaje sólo indica que el administrador de tarjetas no es capaz de asignar un controlador a la tarjeta, ya que los archivos `/etc/pcmcia/config` o `/etc/pcmcia/*.conf` son necesarios para esta asignación. Estos archivos son, por así decirlo, una base de datos de controladores que se puede ampliar fácilmente usando entradas existentes como plantilla para las nuevas. Para identificar la tarjeta, puede emplear el comando `cardctl ident`. Puede obtener más información sobre este tema en el HOWTO de PCMCIA (sección 6) y en la página del manual pcmcia(5). Después de modificar `/etc/pcmcia/config` o `/etc/pcmcia/*.conf`, debe cargar de nuevo la asignación de controladores mediante `rcpcmcia reload`.

El controlador no se carga Una de las causas es que exista una asignación incorrecta en la base de datos de controladores. Esto puede ocurrir por ejemplo si el fabricante ha insertado un chip distinto en un modelo de tarjeta que no ha cambiado externamente. A veces existen controladores opcionales que funcionan mejor (o funcionan solamente) con modelos distintos al controlador especificado. En estos casos se necesita información exacta sobre la tarjeta. También sirve de ayuda preguntar en listas de correo o a nuestro servicio de soporte avanzado.

En el caso de tarjetas CardBus es necesario añadir la entrada `HOTPLUG_DEBUG=yes` al archivo `/etc/sysconfig/hotplug`. De este modo el sistema produce mensajes en el archivo de registro que indican si el controlador ha sido cargado correctamente.

Otra causa puede ser un conflicto de recursos. Aunque para la mayoría de las tarjetas PCMCIA no importa qué IRQ, puerto E/S o rango de memoria se utiliza, existen algunas excepciones. Por eso siempre es necesario probar primero una tarjeta y en ocasiones desconectar además temporalmente otros componentes del sistema como tarjetas de sonido, IrDA, modems o impresoras. Se puede ver la distribución de recursos del sistema con el comando `lsdev` ejecutado como usuario `root`. (Es normal que varios dispo-

sitivos PCI utilicen el mismo IRQ).

Una posible solución consiste en emplear la opción adecuada para el módulo de controladores de tarjeta. Dicha opción se puede averiguar con `modinfo⟨controlador⟩`. Para la mayoría de los módulos existe una página man. El comando `rpm -ql pcmcia | grep man` muestra una lista de todas las páginas man incluidas en el paquete `pcmcia`. Para probar las opciones también es posible descargar los controladores de tarjetas manualmente.

Una vez que el problema esté resuelto, , el uso de un recurso determinado puede permitirse o prohibirse de manera generalizada en el archivo `/etc/pcmcia/config.opts`. Las opciones para los controladores de tarjetas también pueden introducirse en este archivo. Si, por ejemplo, el módulo `pcnet_cs` sólo debe utilizarse con IRQ 5, se debe realizar la siguiente entrada:

```
module pcnet_cs opts irq_list=5
```

Interfaz mal configurada En este caso se recomienda comprobar concienzudamente la configuración de la interfaz y el nombre de la configuración con `getcfg`. Asimismo es necesario asignar el valor `yes` a las variables `DEBUG` en `/etc/sysconfig/network/config` y `HOTPLUG_DEBUG` en `/etc/sysconfig/hotplug`. Con otro tipo de tarjetas o si esto no funciona, existe la posibilidad de incluir una línea `set -x` en el script activado por hotplug o el administrador de tarjetas (ver `/var/log/messages`). De esta forma, cada uno de los comandos del script se recogerán en el registro del sistema. Si encuentra el pasaje problemático en un script, puede introducir y probar los comandos correspondientes en una terminal.

14.6. Información adicional

Si está interesado en el funcionamiento de determinados portátiles, visite el sitio web de Linux Laptop en `http://linux-laptop.net`. Otra buena fuente de información es el sitio web de TuxMobil `http://tuxmobil.org/`. Además de información muy interesante, allí encontrará también un COMO sobre portátiles y otro acerca de IrDA. La base de datos de soporte también contiene varios artículos sobre el uso de portátiles con SUSE LINUX. Puede acceder a ellos introduciendo el término de búsqueda *laptop* o *notebook* en `http://portal.suse.de/sdb/es/index.html`.

SCPM (System Configuration Profile Management)

Este capítulo es una introducción a SCPM (System Configuration Profile Management), un sistema que le permite ajustar la configuración del ordenador a distintos entornos de operación o configuraciones de hardware. SCPM administra un conjunto de perfiles del sistema adaptados a los escenarios de aplicación correspondientes. El simple cambio de un perfil a otro en SCPM sustituye a la modificación manual de la configuración del sistema.

A veces se dan situaciones en las que es necesario modificar la configuración del sistema. Este es sobre todo el caso de 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 que simplemente se quiera probar algo nuevo. En cualquier caso, debería ser fácil volver al sistema de partida y mejor todavía si fuera posible volver a reproducir fácilmente la configuración modificada. System Configuration Profile Management permite configurar una parte de la configuración del sistema de forma que los distintos estados se puedan guardar en un perfil de configuración propio.

El escenario de aplicación principal reside en la configuración de red de los portátiles. Sin embargo, las distintas configuraciones de red influyen en muchos casos en otros elementos, como por ejemplo la configuración del correo electrónico o los proxies. A esto se le añade la configuración de distintas impresoras en casa o en el trabajo, la configuración especial de X.Org para realizar presentaciones con un proyector, los distintos modos de ahorro de energía para cuando se trabaja con baterías o una zona horaria distinta para el extranjero.

15.1. Terminología

A continuación se exponen unos conceptos básicos que se utilizarán en el resto de la documentación sobre SCPM y en el módulo de YaST.

- Por *configuración del sistema* entendemos toda la configuración del ordenador; todas las configuraciones básicas, como por ejemplo las particiones de los discos duros o las configuraciones de red, la selección de zona horaria o la 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 ejecuta en un perfil y está desactivado en otro.

- 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.

15.2. Configuración de SCPM desde la línea de comandos

Esta sección presenta la configuración de SCPM desde la línea de comandos y trata, entre otros temas, el inicio y la configuración de SCPM y el trabajo con perfiles.

15.2.1. Iniciar SCPM y definir los grupos de recursos

Antes de poder trabajar con SCPM hay que iniciarlo, lo que sucede con `scpm enable`. 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.

De manera estándar, SCPM engloba la configuración de redes e impresoras así como la configuración de X.Org 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 como usuario `root`.

```
scpm list_groups -a

nis                 Network Information Service client
mail                Mail subsystem
ntpd                Network Time Protocol daemon
xf86                X Server settings
```

```
autofs              Automounter service
network             Basic network settings
printer             Printer settings
```

Puede activar y desactivar los grupos con `scpm activate_group NAME` o `scpm deactivate_group NAME`. En estos comandos debe sustituir `NAME` por el nombre de grupo correspondiente.

15.2.2. Crear y administrar perfiles

Cuando SCPM se activa, ya existe un perfil denominado `default` (predeterminado). 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 derivará el resto de los perfiles. Por este motivo, primero se deben definir las opciones de configuración que aparecerán en todos los perfiles. `scpm reload` guarda las modificaciones en el perfil activo. Puede copiar y cambiar el nombre del perfil `default` para utilizarlo como base para nuevos perfiles.

Existen dos maneras de crear un perfil. Si, por ejemplo, el nuevo perfil (aquí con el nombre `work`) debe partir del perfil `default`, introduzca `scpm copy default work`. A continuación escriba `scpm switch work` para cambiar al nuevo perfil y configurarlo. En ocasiones se ha modificado la configuración del sistema para un propósito determinado y esta se quiere guardar en un nuevo perfil. Para ello ha de ejecutar `scpm add work`. Ahora, la configuración actual del sistema ha quedado guardada en el perfil `work`, que se marcará como activo. `scpm reload` guarda los cambios en el perfil `work`.

También es posible cambiar el nombre de los perfiles o eliminarlos. Para ello se emplean los comandos `scpm rename x y` y `scpm delete x`. Por ejemplo, para cambiar el nombre de `work` a `trabajo` debe introducirse el comando `scpm rename work trabajo`. Si posteriormente desea borrarlo, utilice el comando `scpm delete trabajo`. El perfil activo no puede borrarse.

15.2.3. Pasar de un perfil de configuración a otro

Para cambiar a otro perfil (aquí llamado `work`) se utiliza el comando `scpm switch work`. Puede cambiar al perfil activo para guardar en él las opciones

modificadas de la configuración del sistema. Esto equivale al comando `scpm reload`.

Al cambiar de perfil, SCPM comprueba primero qué recursos del perfil activo han sido modificados desde el último cambio de un perfil a otro. A continuación pregunta en cada caso si el cambio en el recurso debe añadirse al perfil activo o desecharse. Si en lugar de los grupos de recursos prefiere ver una 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`.

```
scpm switch -r work

Checking for modified resources
Checking for Resources to be started/shut down
Checking for dependencies
Restoring profile default
```

A continuación, SCPM compara la configuración actual del sistema con el perfil 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. Llegado a este momento se detienen los servicios del sistema, se escriben todos los recursos modificados (por ejemplo los archivos de configuración) y se reinician los servicios del sistema.

15.2.4. Configuración avanzada del perfil

Para cada perfil puede introducir una descripción que se muestre al ejecutar `scpm list`. Si desea incluir una descripción para el perfil activo, utilice el comando `scpm set description "texto"`. Para perfiles no activos, debe indicar además el nombre del perfil: `scpm set description 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 distintas fases del proceso de cambio de un perfil a otro. Estas fases son:

prestop antes de parar los servicios al abandonar un perfil

poststop después de parar los servicios al abandonar un perfil

prestart antes de iniciar los servicios al activar un perfil

poststart después de iniciar los servicios al activar un perfil

El comando `set` permite añadir estas acciones con los comandos `scpm set prestop nombre_archivo`, `scpm set poststop nombre_archivo`, `scpm set prestart nombre_archivo` y `scpm set poststart nombre_archivo`. Se debe tratar de un programa ejecutable, es decir, los scripts deben incluir los intérpretes adecuados.

Aviso

Integración de scripts personalizados

El superusuario `root` ha de tener permiso de lectura y ejecución sobre los scripts adicionales que deba ejecutar SCPM mientras que el resto de usuarios no debe poder acceder a estos archivos. Esto se consigue con los comandos `chmod 700 nombre_archivo` y `chown root:root nombre_archivo`.

Aviso

Se pueden consultar 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 `""`, es decir, el comando `scpm set prestop ""` retira el programa poststop.

Es posible aplicar todos los comandos `set` y `get` a cualquier perfil de la misma forma que se añaden las descripciones. Algunos ejemplos de estos comandos son `scpm get prestop nombre_archivo work` o `scpm get prestop work`.

15.3. El gestor de perfiles de YaST

En primer lugar inicie el gestor de perfiles de YaST desde el centro de control de YaST (‘Sistema’ → ‘Gestor de perfiles’). La primera vez que lo inicie, debe activar SCPM explícitamente seleccionando ‘Activado’ en el diálogo de ‘Opciones SCPM’ que se muestra en la figura **??** en esta página. En el apartado ‘Configuración’ puede definir si las ventanas de progreso han de cerrarse automáticamente y si el sistema debe mostrar mensajes detallados sobre el progreso de la configuración de SCPM. En ‘Modo de cambio’ se determina si los recursos modificados del perfil activo deben guardarse o desecharse cuando se cambia de perfil. Si el ‘Modo

de cambio' es 'Normal', todos los cambios del perfil activo se guardan cuando se cambia de perfil. Para definir el comportamiento de SCPM durante el arranque, seleccione en el apartado 'Modo de arranque' la opción 'Guardar los cambios' (predeterminada) o 'Desechar los cambios'.

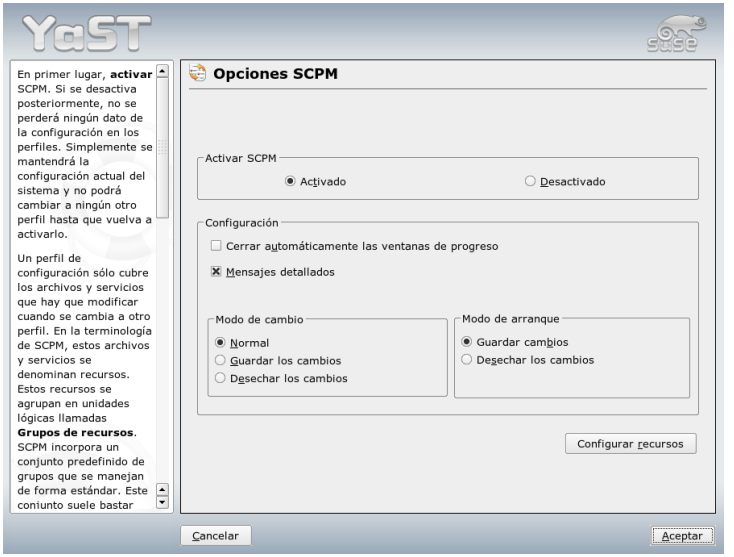

Figura 15.1: *Opciones SCPM en YaST*

15.3.1. Configuración de grupos de recursos

Para modificar la configuración actual de los recursos pulse el botón 'Configurar recursos' en el diálogo 'Opciones SCPM'. En el diálogo que aparece a continuación, 'Configuración de grupos de recursos' (mostrado en la figura **??** en esta página), se muestran todos los grupos de recursos disponibles en el sistema. Para añadir o editar un grupo de recursos, edite o defina el 'Grupo de recursos' y la 'Descripción'. Por ejemplo, para un servicio LDAP introduzca `ldap` como 'Grupo de recursos' y `Servicio para cliente LDAP` como 'Descripción'. A continuación añada los recursos apropiados (servicios, archivos de configuración o ambos) o modifique los recursos existentes. También puede borrar aquellos

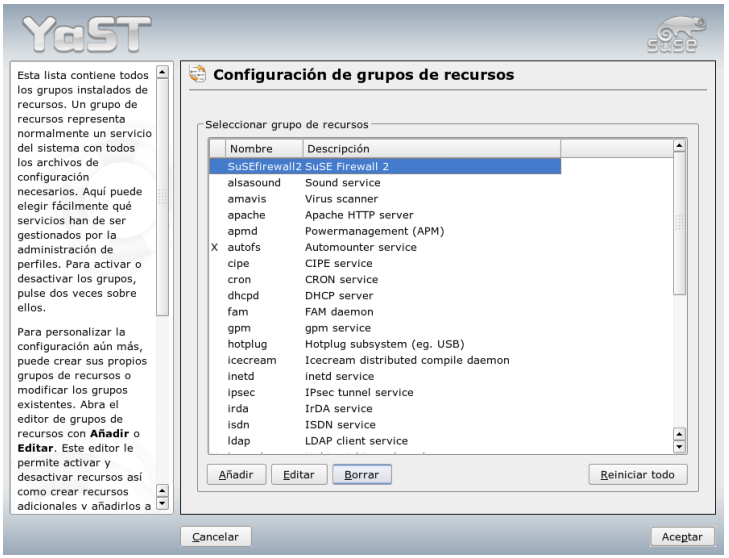

Figura 15.2: *Configuración de grupos de recursos*

que no se usan. Para devolver los recursos seleccionados a su estado original, desechando los cambios realizados y restableciendo los valores predeterminados, pulse el botón 'Reiniciar grupo'. Los cambios se guardarán en el perfil activo.

15.3.2. Creación de un nuevo perfil

Puede crear un nuevo perfil pulsando en el botón 'Añadir' en el diálogo de inicio ('Gestión de perfiles de la configuración del sistema'). Seleccione en la ventana que se abre a continuación si el nuevo perfil ha de estar basado en la configuración actual del sistema (SCPM obtiene automáticamente la configuración existente y la escribe en el perfil) o en un perfil ya existente. Si escoge la configuración actual del sistema como base del nuevo perfil, puede seleccionarlo como nuevo perfil activo. No se ocasionará ningún cambio en el perfil antiguo ni se iniciarán o detendrán servicios.

Introduzca el nombre y una breve descripción del nuevo perfil en el siguiente diálogo. Si desea que SCPM ejecute scripts especiales al cambiar de perfil, intro-

duzca las rutas a todos los ejecutables (ver figura **??** en esta página). Puede obtener información adicional en la sección **??** en esta página. Finalmente, SCPM prueba los recursos del nuevo perfil y, si esta comprobación resulta satisfactoria, el nuevo perfil está listo para el uso.

Figura 15.3: *Configuraciones especiales de perfiles*

15.3.3. Modificación de perfiles existentes

Para modificar un perfil existente, seleccione 'Editar' en el diálogo de inicio ('Gestión de perfiles de la configuración del sistema') y realice los cambios deseados en el nombre, descripción, scripts y recursos.

15.3.4. Cambio de perfil

Puede cambiar de perfil desde el menú de inicio. El perfil activo está marcado con una flecha. Para cambiar de perfil, seleccione el perfil al que desea cambiar y pulse 'Cambiar a'. SCPM comprueba la existencia de recursos nuevos o modificados y los añade en caso necesario.

Si se ha modificado un recurso, YaST abre el diálogo 'Confirmar cambio'. Bajo el epígrafe 'Recursos modificados del perfil activo' se muestran todos los grupos de recursos del perfil activo que se han modificado pero todavía no se han guardado en el mismo. El botón 'Guardar o ignorar' le permite guardar en el perfil activo los cambios en el grupo de recursos seleccionado (en ese caso aparece una X a la izquierda del recurso) o bien desecharlos. También es posible seleccionar un recurso y pulsar en 'Detalles' para un análisis exhaustivo de los cambios. Al hacerlo se muestra una lista con todos los archivos de configuración o ejecutables que pertenecen a ese grupo de recursos y han sido modificados. Para obtener una comparación línea por línea entre la versión nueva y la antigua, pulse 'Mostrar los cambios'. Una vez analizados los cambios, decida qué hacer con ellos seleccionando una 'Acción':

Guardar recurso Guardar este recurso en el perfil activo pero sin modificar el resto de perfiles.

Ignorar recurso No modificar el recurso activo actualmente. El cambio se desecha.

Guardar en todos los perfiles Copiar la configuración de este recurso en el resto de perfiles.

Parchear en todos los perfiles Aplicar sólo los últimos cambios a todos los perfiles.

'Guardar o ignorar todo' guarda o desecha los cambios en todos los recursos de la lista.

Después de confirmar los cambios en el perfil activo, pulse 'OK' para salir del diálogo 'Confirmar cambio'. SCPM cambia entonces de perfil y en el proceso ejecuta los scripts prestop y poststop del antiguo perfil y los scripts prestart y poststart del nuevo perfil.

15.4. Posibles problemas y sus soluciones

Esta sección describe algunos problemas frecuentes en conexión con SCPM. Sepa por qué se producen y cómo pueden resolverse.

15.4.1. Interrupción durante el proceso de cambio

En algunos casos, SCPM se interrumpe de forma repentina durante el proceso de 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. En cualquier caso, al intentar reiniciar SCPM obtendrá un mensaje de error que le informa de 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 del sistema. Para resolver el problema ejecute `scpm recover` para que SCPM lleve a cabo todas las operaciones que no se han realizado en la ejecución anterior. También puede ejecutar `scpm recover -b`, que intenta deshacer todas las operaciones efectuadas en la ejecución anterior. Si está utilizando el gestor de perfiles de YaST, durante el inicio obtendrá un diálogo de recuperación donde puede ejecutar estos comandos.

15.4.2. Cambio en la configuración de un grupo de recursos

Si desea modificar la configuración de un grupo de recursos una vez que se ha iniciado SCPM, ejecute el comando `scpm rebuild` cuando haya terminado de añadir o eliminar grupos. Este comando se encarga de añadir nuevos recursos a todos los perfiles y eliminar definitivamente los recursos borrados. Si ha configurado los recursos borrados de forma distinta en los diversos perfiles, perderá estos datos de configuración (excepto la versión actual de los datos en su sistema, que no se ve modificada por SCPM). Si edita la configuración con YaST no es necesario que ejecute ningún comando rebuild; YaST se ocupa de ello automáticamente.

15.5. Selección de un perfil durante el arranque

Para seleccionar un perfil durante el arranque del sistema, pulse (F4) en la pantalla de arranque a fin de acceder a una lista de los perfiles disponibles. Utilice las teclas de cursor para seleccionar el perfil y confirme la selección con (Intro). El perfil seleccionado se utilizará como opción de arranque.

15.6. Información adicional

La documentación más actual se recoge en la página info de SCPM. Puede visualizar esta página con programas como Konqueror o Emacs (`konqueror info:scpm`) o bien utilizar los comandos `info` o `pinfo` en la línea de comandos. La información específica para desarrolladores se encuentra en `/usr/share/doc/packages/scpm`.

Gestión de energía

Este capítulo le presenta las distintas técnicas de gestión de energía en Linux y describe con detalle la configuración de las más importantes, como por ejemplo APM (Advanced Power Management), ACPI (Advanced Configuration and Power Interface) o los ajustes de frecuencia de la CPU (CPU Frequency Scaling).

En este campo se ha evolucionado desde la mera gestión de energía en portátiles por medio de APM hasta ACPI, que constituye una herramienta de información y configuración de hardware disponible en todos los ordenadores de fabricación reciente (portátiles, equipos de sobremesa y servidores). Asimismo, en muchas clases de hardware moderno es posible adaptar la frecuencia de la CPU a la situación correspondiente (*CPU Frequency Scaling*), lo que reduce el consumo de la batería en los dispositivos móviles.

Todas las técnicas de gestión de energía (power management) requieren un hardware y una rutina de la BIOS apropiados. La mayoría de los ordenadores portátiles y muchos ordenadores de sobremesa y servidores cumplen estos requisitos. En el hardware más antiguo se utiliza con frecuencia el estándar APM (Advanced Power Management). Debido a que APM consiste básicamente en un conjunto de funciones implementadas en la BIOS, existen diferencias en el soporte de APM en las distintas clases de hardware. ACPI es todavía más complejo y la calidad de su soporte depende incluso en mayor medida del hardware utilizado. Por este motivo no tiene mucho sentido abogar por uno u otro sistema. Le aconsejamos probar en su hardware las distintas técnicas posibles y optar por la que mejor soporte tenga.

Importante

Gestión de energía en procesadores AMD64

Los procesadores AMD64 con un kernel de 64 bits soportan exclusivamente ACPI.

Importante

16.1. Funciones para el ahorro de energía

Las funciones de ahorro de energía no sólo desempeñan un papel importante en en conexión con los ordenadores portátiles, sino también con los sistemas de sobremesa. A continuación se describen brevemente las funciones más importantes así como su uso en los sistemas de gestión de energía APM y ACPI:

Standby (en reposo) Se desactiva la pantalla y en algunos dispositivos se reduce también el rendimiento del procesador. No todas las implementaciones APM ofrecen esta función. En ACPI este estado se corresponde con S1 o S2.

Suspend (to memory) Este modo guarda toda la información sobre el estado del sistema en la memoria. A continuación, todo el sistema con excepción de ésta se para. Es un estado en el cual el ordenador gasta muy poca energía. Su gran ventaja es que permite reanudar en unos pocos segundos el trabajo donde lo habíamos dejado sin necesidad de arrancar y cargar de nuevo los programas usados. En la mayoría de los dispositivos con APM basta con cerrar la tapa para suspender y abrirla después para seguir trabajando. En *ACPI* este estado se corresponde con *S3*. El soporte de este estado depende enormemente del hardware utilizado.

Hibernation (suspend to disk) En este modo, el contenido de la memoria se guarda en el disco duro y a continuación el sistema se apaga. El ordenador tarda de treinta a noventa segundos en salir de este periodo de hibernación, tras lo cual se restablece por completo el estado anterior al suspend. Algunos fabricantes ofrecen ciertos modos híbridos (por ejemplo RediSafe en IBM Thinkpads). En *ACPI* el estado de hibernación se corresponde con *S4*. En Linux, el modo *Suspend to disk* es ejecutado por rutinas del kernel independientes de APM y ACPI.

Control de batería Tanto ACPI como APM controlan el nivel de carga de la batería e informan sobre el nivel de carga actual. Asimismo, ambos sistemas coordinan la ejecución de determinadas acciones cuando se alcanza un nivel de carga crítico.

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 agote la batería.

Apagado de los componentes del sistema
El componente que ahorra una mayor energía al apagarse es el disco duro. Dependiendo de la fiabilidad del sistema, este se puede poner a dormir 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.

Control del rendimiento del procesador
Existen tres formas de ahorro de energía en conexión con el procesador. El ajuste de la frecuencia y el voltaje (también llamado PowerNow! o Speedstep), la suspensión del reloj de CPU (throttling) y la inactividad del

procesador (estados C). Estos tres métodos pueden combinarse de la forma más apropiada según el modo de operación del ordenador.

16.2. 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 hace falta que se ejecuten ciertas acciones antes de pasar al modo de suspensión. Para mostrar el nivel de carga de la batería, es necesario contar con determinados paquetes y un kernel apropiado.

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`.

Debido a que no todas las implementaciones BIOS cumplen el estándar APM al cien por cien, pueden producirse problemas al utilizar APM. Algunos de estos problemas se pueden resolver con parámetros especiales. Todos los parámetros se introducen en el prompt de arranque con la forma `apm=<parámetro>`:

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 función GetPowerStatus de la BIOS no funciona correctamente.

(no-)realmode-power-off Pasa el procesador al modo real 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 o `idle` (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 de APM (apmd) que se utilizaba anteriormente ha dejado de emplearse. Sus funciones están incluidas en el nuevo powersaved, que también domina ACPI y el ajuste de frecuencia de la CPU.

16.3. ACPI

ACPI significa 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. Asimismo, ACPI proporciona diversos datos sobre la batería, interfaz de red, temperatura y ventilador e informa de acontecimientos en el sistema como ”Cerrar la cubierta” o ”Baterías poco cargadas”.

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. Para obtener más información sobre la resolución de problemas en ACPI consulte la sección **??** en esta página.

16.3.1. 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`.

A continuación es necesario cargar una serie de módulos, 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/powersave/`

`common`. 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 algunos de estos estados. No todas las funciones se soportan completamente ya que algunas se encuentran todavía en desarrollo y el soporte de otras depende en gran medida de la implementación del fabricante.

`cat` muestra todos los archivos (excepto `dsdt` y `fadt`). En algunos se puede incluso modificar opciones pasando a X valores adecuados con `echo`, por ejemplo `echo X > <archivo>`. Para acceder a esta información y a las posibilidades de control se recomienda utilizar siempre el comando `powersave`. No obstante, para lograr una mejor comprensión de ACPI 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. El soporte actual de esta función es insuficiente.

`/proc/acpi/sleep` Proporciona información sobre los posibles estados de sueño.

`/proc/acpi/event` Aquí se registran los eventos del sistema. Estos son procesados por el daemon de Powersave (`powersaved`). Si no interviene ningún daemon, los eventos de pueden leer con `cat /proc/acpi/event` (salir con Ctrl + C). Un ejemplo de evento es pulsar el interruptor principal o cerrar el portátil.

`/proc/acpi/dsdt` y `/proc/acpi/fadt`
Aquí se almacenan las tablas ACPI DSDT (*Differentiated System Description Table*) y FADT (*Fixed ACPI Description Table*). Estas pueden leerse con `acpidmp`, `acpidisasm` y `dmdecode`. Puede encontrar estos programas junto con la correspondiente documentación en el paquete `pmtools`. Por ejemplo: `acpidmp DSDT | acpidisasm`.

`/proc/acpi/ac_adapter/AC/state`
Muestra si el adaptador de red está conectado.

`/proc/acpi/battery/BAT*/{alarm,info,state}`
Contienen abundante información sobre el nivel 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 como los descritos en la sección **??** en esta página. En `alarm` se puede introducir qué nivel de carga provocará un evento en la batería.

`/proc/acpi/button` Este directorio contiene información sobre diversos interruptores.

`/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) sobreescriben estos valores cuando la temperatura es demasiado elevada.

`/proc/acpi/processor/CPU*/info`
Información sobre las posibilidades de ahorro de energía del procesador.

`/proc/acpi/processor/CPU*/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/CPU*/throttling`
Aquí se puede configurar la suspensión del reloj de la CPU. Normalmente es posible reducirlo en ocho fases. Esta opción es independiente del control de frecuencia de la CPU.

`/proc/acpi/processor/CPU*/limit`
Si un daemon se encarga de regular automáticamente el rendimiento (obsoleto) y el throttling, aquí se pueden definir los límites que no se deben sobrepasar en ningún caso. Existen algunos límites que fija el sistema y otros que fija el usuario.

`/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, algunas de las descripciones ofrecidas a continuación tienen un valor puramente teórico.

/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
: Aquí se puede seleccionar el método de refrigeración controlado por ACPI: pasivo (menor rendimiento, económico) o activo (máximo rendimiento, ruidoso a causa del ventilador).

/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`). Las acciones posibles se encuentran definidas en DSDT en función del dispositivo. Los `trip points` definidos en la especificación ACPI son: `critical`, `hot`, `passive`, `active1` y `active2`. Aunque no siempre estén implementados todos, han de introducirse en este orden cuando se escriba en el archivo `trip_points`. Por ejemplo, la entrada `echo 90:0:70:0:0 > trip_points` asigna a la temperatura un valor `critical` de `90` y un valor `passive` de `70` grados centígrados.

/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`.

Los datos, opciones de configuración y eventos mencionados en las líneas superiores no tienen que editarse manualmente. Para ello cuenta con el daemon de Powersave (powersaved) y con diversos programas como powersave, kpowersave y wmpowersave (vea la sección **??** en esta página). Puesto que las prestaciones del antiguo acpid se han incluido en powersaved, acpid ha quedado obsoleto.

16.3.2. Control de la potencia del procesador

Existen tres métodos de ahorro de energía para el procesador que pueden combinarse en función del modo de operación del ordenador. El ahorro de energía

también significa que el sistema se calienta menos y por tanto el ventilador debe activarse con menor frecuencia.

Ajuste de la frecuencia y el voltaje PowerNow! y Speedstep son los nombres dados por las empresas AMD e Intel a esta técnica que también existe en procesadores de otros fabricantes. Este método consiste en reducir conjuntamente el reloj de la CPU y su voltaje central. La ventaja es un ahorro de energía superior al lineal. Esto significa que con la mitad de la frecuencia (es decir, la mitad de la potencia) se requiere mucho menos de la mitad de energía. Esta técnica funciona independientemente de APM o ACPI y requiere un daemon que ajuste la frecuencia a los requisitos de potencia actuales. La configuración puede realizarse en el directorio `/sys/devices/system/cpu/cpu*/cpufreq/`.

Suspensión del reloj de CPU Este método se conoce como throttling ("estrangulamiento") y consiste en omitir un porcentaje determinado del impulso de la señal de reloj para la CPU. Con una reducción del 25 % se omite uno de cada cuatro impulsos mientras que con una reducción del 87,5 %, solamente uno de cada ocho impulsos llega al procesador. No obstante, el ahorro de energía es algo menor que el lineal. La técnica de throttling se utiliza solamente cuando no existe el ajuste de la frecuencia o para lograr el máximo ahorro. Esta técnica también requiere un proceso propio que la controle. La interfaz del sistema es `/proc/acpi/processor/*/throttling`.

Inactividad del procesador El sistema operativo pone al procesador en un estado de sueño o inactividad cuando no hay nada que hacer. En este caso, el sistema operativo envía al procesador la instrucción `halt`. Existen distintos niveles: C1, C2 y C3. En el estado de máximo ahorro de energía, C3, se detiene incluso la sincronización de la caché del procesador con la caché de la memoria principal, por lo que este estado se adopta únicamente cuando no existe ningún dispositivo que modifique el contenido de la memoria principal a través de la actividad bus master. Por este motivo, algunos controladores no permiten el uso de C3. El estado actual se muestra en `/proc/acpi/processor/*/power`.

La reducción de frecuencia y la supresión de señales son relevantes cuando el procesador está activo, ya que si no está realizando acción ninguna se utilizan preferentemente los estados C.

Si la CPU está ocupada, la reducción de la frecuencia es el mejor método para ahorrar energía. Con mucha frecuencia el procesador no trabaja al máximo de su

capacidad y basta con bajar su frecuencia. En la mayoría de los casos, el método más adecuado consiste en un ajuste dinámico de la frecuencia por medio de un daemon (por ejemplo powersaved). Cuando el ordenador funciona con baterías o debe mantener una baja temperatura y hacer poco ruido, se recomienda asignar de forma permanente una frecuencia baja.

El throttling debería utilizarse como último recurso. Por ejemplo, cuando queremos prolongar lo más posible el tiempo de vida de las baterías con el procesador trabajando al máximo de su capacidad. No obstante, algunos sistemas ya no funcionan correctamente si el nivel de throttling es demasiado elevado. La supresión de la señal de reloj de la CPU no sirve de nada cuando la carga de trabajo del procesador es baja.

En SUSE LINUX, estas técnicas se controlan a través del daemon de Powersave. La configuración necesaria se describe en la sección **??** en esta página.

16.3.3. Herramientas ACPI

Existe una serie de herramientas ACPI más o menos completas. Entre ellas se encuentran herramientas puramente informativas que muestran el nivel 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`).

16.3.4. Posibles problemas y sus 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. 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.

Aviso

Problemas al arrancar sin ACPI

Algunos ordenadores de última generación, especialmente los sistemas SMP y AMD64M, requieren ACPI para que el hardware se configure correctamente. Por lo tanto, el desactivar ACPI puede ocasionar problemas.

Aviso

Examine los mensajes de arranque cuidadosamente. Utilice para ello 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 pasar una versión mejorada al sistema. De esta forma la tabla DSDT incorrecta de la BIOS será ignorada. El proceso correspondiente se describe en la sección **??** en esta página.

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. Precisamente porque los fabricantes no siempre ayudan cuando se trata de Linux, es importante que tomen conciencia de los posibles problemas. 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 hardware de que lo usa con Linux.

Información adicional

Puede obtener información adicional y material de ayuda sobre ACPI (en inglés) en:

- `http://www.cpqlinux.com/acpi-howto.html` (HOWTO para ACPI, 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://www.poupinou.org/acpi/` (parches DSDT de Bruno Ducrot)

16.4. Parar el disco duro

En Linux es posible parar el disco duro completamente cuando no se necesita o hacer que funcione en modo silencioso o de ahorro de energía. La desactivación a tiempo parcial de los discos no merece la pena en los portátiles modernos, ya que los discos adoptan por sí mismos el modo de ahorro de energía cuando no se necesitan. Quien desee ahorrar el máximo de energía puede probar alguna de las posibilidades que se describen a continuación. La mayor parte de las prestaciones pueden controlarse con powersaved.

El programa hdparm se utiliza para definir opciones de configuración en el disco duro. La opción `-y` pone el disco duro inmediatamente en modo de reposo, mientras que `-Y` (¡cuidado!) lo para completamente. Con `hdparm -S <x>` se consigue que el disco duro se apague tras un determinado período de inactividad. La posición $\langle x \rangle$ posee los siguientes 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.

Las posibilidades internas de ahorro de energía en el disco se controlan por medio de la opción `-B`. Aquí puede seleccionarse desde un ahorro máximo hasta un rendimiento máximo a través de un número entre `0` y `255`. El resultado depende del disco utilizado y es difícil de juzgar. Para que el disco duro sea más silencioso puede utilizarse la opción `-M`. Aquí también se elige un número entre `128` y `254` para definir un estado entre silencioso y rápido.

Sin embargo a menudo no es tan sencillo parar el disco duro 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 antigüedad 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.

Aviso

Peligro para la seguridad de los datos

Las modificaciones en la configuración del Kernel Update Daemon pueden poner en peligro la seguridad de los datos.

Aviso

Además de todo lo anterior, los denominados sistema de archivos Journaling o transaccionales como por ejemplo 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. por ejemplo 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. Si desea averiguar qué proceso está escribiendo en el disco en un momento determinado, puede activar el modo de depuración con el comando `echo 1 > /proc/sys/vm/block_dump`. Esto hace que se registren todas las actividades del disco en el archivo de registro del sistema. El modo de depuración se desactiva asignándole en el archivo el valor `0`.

En este contexto, el daemon de correo postfix dispone de una variable llamada `POSTFIX_LAPTOP`. Cuando esta variable contiene el valor `yes`, postfix accede con mucha menos frecuencia al disco duro. No obstante, esto carece de importancia si el intervalo de kupdated ha sido ampliado.

16.5. El paquete powersave

El paquete `powersave` se ocupa de la función de ahorro de energía cuando un portátil funciona en el modo de batería. No obstante, algunas de sus funciones resultan también muy interesantes para estaciones de trabajo o servidores, como por ejemplo el modo suspend/standby, la función de las teclas ACPI y la activación o desactivación automática de discos duros IDE.

Este paquete incorpora todas las funciones de gestión de energía del ordenador y soporta cualquier hardware que utilice ACPI, APM, discos IDE y las tecnologías PowerNow! o SpeedStep. `powersave` agrupa todas las prestaciones de los paquetes `apmd`, `acpid`, `ospmd` y `cpufreqd` (actualmente `cpuspeed`). Los daemons de estos paquetes no deben ejecutarse de forma paralela al daemon de powersave.

Incluso aunque el sistema no disponga de todos los componentes de hardware mencionados arriba (APM y ACPI se excluyen mutuamente), se recomienda utilizar el daemon de powersave para regular la función de ahorro de energía. Este daemon detecta automáticamente cualquier cambio en la configuración del hardware.

Importante

Información sobre powersave

Puede obtener información adicional sobre el paquete powersave en `/usr/share/doc/packages/powersave`.

Importante

16.5.1. Configuración del paquete powersave

En general, la configuración de powersave está distribuida en varios archivos:

`/etc/sysconfig/powersave/common`
: Este archivo contiene opciones de configuración general para el daemon de powersave. Aquí se puede definir, por ejemplo, la cantidad de mensajes de depuración (en `/var/log/messages`) a través del valor asignado a la variable `POWERSAVE_DEBUG`.

`/etc/sysconfig/powersave/events`
: El daemon de powersave requiere este archivo para procesar los sucesos

(events) que se producen en el sistema. A estos sucesos se les puede asignar acciones externas o internas (ejecutadas por el daemon). Se habla de una acción externa cuando el daemon intenta activar un archivo ejecutable guardado en `/usr/lib/powersave/scripts/`. En cuanto a las acciones internas predefinidas, son las siguientes:

- ignore
- throttle
- dethrottle
- suspend_to_disk
- suspend_to_ram
- standby
- do_suspend_to_disk
- do_suspend_to_ram
- do_standby

`throttle` ralentiza el procesador en la medida definida en `POWERSAVE_MAX_THROTTLING`. El valor asignado a esta variable depende del perfil usado en ese momento. `dethrottle` hace que el procesador recupere su máxima potencia. `suspend_to_disk`, `suspend_to_ram` y `standby` provocan el evento del sistema para el modo `sleep`. Las tres últimas acciones se ocupan en general de desencadenar el modo `sleep`, pero siempre deben asignarse a eventos del sistema concretos.

Los scripts para ejecutar los eventos se encuentran en el directorio `/usr/lib/powersave/scripts`:

notify Notificación por medio de la consola, X Window o una señal acústica de que se ha producido un evento.

screen_saver Activa el salvapantallas.

switch_vt Muy útil si la imagen está distorsionada tras un suspend/standby.

wm_logout Guardar la configuración y cerrar la sesión de GNOME, KDE u otro gestor de ventanas.

wm_shutdown Guardar la configuración de GNOME o KDE y apagar el sistema.

Si por ejemplo se han asignado los siguientes valores a la variable `POWERSAVE_EVENT_GLOBAL_SUSPEND2DISK="prepare_suspend_-to_disk do_suspend_to_disk"`, tan pronto como el usuario dé a powersaved la orden para el modo `Suspend to disk`, se ejecutarán los scripts o acciones especificados en el mismo orden en el que aparecen. El daemon inicia el script externo `/usr/lib/powersave/scripts/prepare_suspend_to_disk` y, una vez que este se ha ejecutado correctamente, realiza la acción interna `do_suspend_to_disk`. Esto significa que el daemon pone al ordenador definitivamente en modo `sleep` después de que el script haya descargado los módulos y detenido los servicios críticos.

A continuación un ejemplo de una acción modificada para el hecho de pulsar un botón (sleep): `POWERSAVE_EVENT_BUTTON_SLEEP="notify suspend_to_disk"`. En este caso se informa al usuario sobre el suspend mediante el script externo `notify`. A continuación se produce el evento `POWERSAVE_EVENT_GLOBAL_SUSPEND2DISK` que origina las acciones mencionadas arriba y garantiza que el sistema pase al modo suspend.

El script `notify` puede personalizarse por medio de la variable `POWERSAVE_NOTIFY_METHOD` en el archivo `/etc/sysconfig/powersave/common`.

`/etc/sysconfig/powersave/cpufreq`
Este archivo contiene variables para optimizar el ajuste dinámico de la frecuencia de la CPU.

`/etc/sysconfig/powersave/battery`
En él se definen los límites de las baterías y otras opciones de configuración específicas de la batería.

`/etc/sysconfig/powersave/sleep`
En este archivo puede definir qué módulos deben descargarse y qué servicios detenerse antes de pasar al modo `sleep`. Estos módulos y archivos serán cargados e iniciados de nuevo cuando el sistema se restablezca. El archivo le permite también retrasar un modo `sleep` desencadenado para, por ejemplo, poder guardar archivos modificados. Las opciones predeterminadas afectan sobre todo a los módulos USB y PCMCIA. Si el cambio a los modos suspend o standby falla, la causa suele estar en ciertos módulos concretos. En la sección ?? en esta página puede encontrar información adicional sobre cómo aislar e identificar el error.

`/etc/sysconfig/powersave/thermal`
Aquí se activa el control para el ajuste del calor y la refrigeración.

Puede obtener información adicional sobre este tema en el archivo `/usr/share/doc/packages/powersave/README.thermal`.

`/etc/sysconfig/powersave/scheme_*`
Este archivo contiene los esquemas o perfiles que regulan el ajuste del consumo de energía en función de los distintos escenarios de aplicación. Algunos de estos perfiles están ya preconfigurados y pueden utilizarse sin más. Aquí también puede almacenar perfiles personalizados.

16.5.2. Configuración de APM y ACPI

Suspend y Standby

Los modos `sleep` están desactivados por defecto ya que todavía fallan en algunos ordenadores. Básicamente existen tres modos `sleep` ACPI y dos APM:

Suspend to Disk (ACPI S4, APM suspend)
Guarda el contenido de la memoria en el disco duro. El ordenador se apaga completamente y no consume electricidad.

Suspend to RAM (ACPI S3, APM suspend)
Guarda los estados de todos los dispositivos en la memoria principal. Sólo la memoria principal consume electricidad.

Standby (ACPI S1, APM standby) Apaga algunos dispositivos en función del fabricante.

Asegúrese que las siguientes opciones predeterminadas están definidas correctamente en el archivo `/etc/sysconfig/powersave/events` para que los modos suspend/standby o resume puedan procesarse adecuadamente (los valores son los predeterminados tras la instalación de SUSE LINUX):

```
POWERSAVE_EVENT_GLOBAL_SUSPEND2DISK=
    "prepare_suspend_to_disk do_suspend_to_disk"
POWERSAVE_EVENT_GLOBAL_SUSPEND2RAM=
    "prepare_suspend_to_ram do_suspend_to_ram"
POWERSAVE_EVENT_GLOBAL_STANDBY=
    "prepare_standby do_standby"
POWERSAVE_EVENT_GLOBAL_RESUME_SUSPEND2DISK=
    "restore_after_suspend_to_disk"
POWERSAVE_EVENT_GLOBAL_RESUME_SUSPEND2RAM=
    "restore_after_suspend_to_ram"
POWERSAVE_EVENT_GLOBAL_RESUME_STANDBY=
    "restore_after_standby"
```

Estados de la batería definidos por el usuario

En el archivo `/etc/sysconfig/powersave/battery` puede definir tres estados de carga de la batería (expresados en forma de porcentaje). Cuando se alcanzan dichos estados, el sistema avisa al usuario o lleva a cabo una acción determinada.

```
POWERSAVED_BATTERY_WARNING=20
POWERSAVED_BATTERY_LOW=10
POWERSAVED_BATTERY_CRITICAL=5
```

En el archivo de configuración `/etc/sysconfig/powersave/events` se definen las acciones/scripts que han de ejecutarse cuando se rebasa un determinado nivel de carga. En la sección **??** en esta página se describe cómo cambiar las acciones predeterminadas para los botones.

```
POWERSAVE_EVENT_BATTERY_NORMAL="ignore"
POWERSAVE_EVENT_BATTERY_WARNING="notify"
POWERSAVE_EVENT_BATTERY_LOW="notify"
POWERSAVE_EVENT_BATTERY_CRITICAL="wm_shutdown"
```

Ajuste del consumo de energía en función de las condiciones de trabajo

Es posible hacer que el funcionamiento del sistema dependa directamente de la forma de suministro de energía. Así por ejemplo, el consumo de energía puede reducirse al utilizar el sistema con baterías y, a la inversa, el rendimiento del sistema puede aumentar de manera automática en cuanto se conecte de nuevo a la red de suministro eléctrico. Entre los parámetros sobre los que se puede influir directamente cabe destacar la frecuencia de la CPU y la función de ahorro de energía de los discos IDE.

Tal y como se define en el archivo `/etc/sysconfig/powersave/events`, el script `powersave_proxy` se encarga de ejecutar determinadas acciones al conectar/desconectar el ordenador a la red eléctrica. En `/etc/sysconfig/powersave/common` puede definir los escenarios (denominados ”perfiles” o ”schemes”) que deben utilizarse:

```
POWERSAVE_AC_SCHEME="performance"
POWERSAVE_BATTERY_SCHEME="powersave"
```

Los perfiles se almacenan en diversos archivos del directorio `/etc/sysconfig/powersave`. Su nombre está formado por `scheme_<nombre_perfil>`. En el

ejemplo se hace referencia a dos perfiles: `scheme_performance` y `scheme_powersave`. Los perfiles `performance`, `powersave`, `presentation` y `acoustic` están ya preconfigurados. El módulo de gestión de energía de YaST (véase la sección **??** en esta página) le permite editar o borrar perfiles ya existentes, crear nuevos perfiles o modificar la correspondencia entre los perfiles y las formas de suministro de energía.

16.5.3. Prestaciones adicionales de ACPI

En caso de que utilice ACPI, puede controlar la reacción del sistema a las *teclas ACPI* (power, sleep, cubierta abierta o cubierta cerrada). En el archivo `/etc/sysconfig/powersave/events` se define la ejecución de las acciones correspondientes. Puede obtener información adicional sobre cada una de las opciones posibles en este archivo de configuración.

POWERSAVE_EVENT_BUTTON_POWER="wm_shutdown"
Al pulsar la tecla power, el sistema apaga el gestor de ventanas correspondiente (KDE, GNOME, fvwm...).

POWERSAVE_EVENT_BUTTON_SLEEP="suspend_to_disk"
Si se pulsa la tecla sleep, el sistema pasa a modo suspend-to-disk.

POWERSAVE_EVENT_BUTTON_LID_OPEN="ignore"
La apertura de la tapa del portátil no provoca ninguna reacción.

POWERSAVE_EVENT_BUTTON_LID_CLOSED="screen_saver"
Al cerrar la tapa del portátil se activa el salvapantallas.

Si el uso del procesador no sobrepasa un nivel determinado durante un periodo de tiempo definido, puede reducir todavía más su potencia. Para ello, defina en `POWERSAVED_CPU_LOW_LIMIT` el nivel de uso que el procesador no debe rebasar durante un periodo de tiempo determinado (que puede especificar en `POWERSAVED_CPU_IDLE_TIMEOUT`) para que se reduzca la potencia de la CPU.

16.5.4. Posibles problemas y sus soluciones

Todos los mensajes de error y avisos del sistema se recogen en el archivo `/var/log/messages`. Si a primera vista tampoco encuentra aquí la causa del problema, asigne el valor `7` o incluso `15` a la variable `DEBUG` en el archivo `/etc/`

`sysconfig/powersave/common` y reinicie el daemon para que los mensajes de powersave sean más extensos e informativos. Al hacerlo, los mensajes de error en `/var/log/messages` serán algo más detallados, lo que le ayudará a identificar el problema. La sección siguiente cubre los problemas más frecuentes que pueden aparecer en relación con powersave.

A pesar de estar activado y con soporte de hardware, ACPI no funciona

Si surgen problemas con ACPI, utilice el comando `dmesg|grep -i acpi` para buscar los mensajes relacionados con ACPI en la salida de `dmesg`.

Para solucionar el error puede ser necesario actualizar la BIOS. Con este fin visite la página web del fabricante del portátil, busque una versión actual de la BIOS e instálela. Informe al fabricante de su sistema de que debe observar la especificación actual de ACPI.

Si el fallo sigue ocurriendo después de actualizar la BIOS, busque en las siguientes páginas web un DSDT más actual para sustituir la tabla DSDT de su sistema, la cual parece estar defectuosa:

1. Descargue de `http://acpi.sourceforge.net/dsdt/tables` un DSDT adecuado para su sistema y asegúrese de que el archivo está descomprimido y compilado (lo reconocerá por la extensión `.aml`, ACPI Machine Language, del archivo). Si este es el caso, pase al punto 3.

2. Si la extensión del archivo descargado es `.asl` (ACPI Source Language), debe compilarlo con la herramienta iasl incluida en el paquete `pmtools`. Para ello ejecute el comando `iasl -sa <nombre_archivo>.asl`. La versión más actual de iasl (Intel ACPI Compiler) está disponible en `http://developer.intel.com/technology/iapc/acpi/downloads.htm`.

3. Copie el archivo `DSDT.aml` a su sistema (por ejemplo a `/etc/DSDT.aml`). A continuación edite `/etc/sysconfig/kernel` y modifique la ruta del archivo DSDT en caso necesario. Inicie `mkinitrd` (paquete `mkinitrd`). Cuando desinstale el kernel y utilice `mkinitrd` para crear un initrd, el nuevo DSDT será integrado y cargado durante el arranque.

CPU Frequency no funciona

Compruebe por medio de las fuentes del kernel (paquete `kernel-source`) si el procesador está soportado y si debe utilizar un módulo del kernel u opción de

módulo específicos para activar la frecuencia de la CPU. Esta información está disponible en `/usr/src/linux/Documentation/cpu-freq/*`. En caso de que sea necesario emplear un módulo u opción determinados, configúrelo en las variables `CPUFREQD_MODULE` y `CPUFREQD_MODULE_OPTS` del archivo `/etc/sysconfig/powersave/cpufreq`.

Los modos suspend/standby no funcionan

Se conocen varios problemas relacionados con el kernel que pueden ser causa de que el modo suspend/standby no funcione en sistemas **ACPI**:

- Los sistemas con más de 1 GB de RAM no soportan (todavía) el modo suspend.
- Los sistemas con multiprocesador o con un procesador P4 (con hyperthreading) no soportan actualmente el modo suspend.

El problema también puede deberse a una implementación defectuosa del DSDT (BIOS). En este caso instale un nuevo DSDT como se ha descrito anteriormente .

En sistemas ACPI y APM, cuando el sistema trata de descargar módulos defectuosos, el ordenador se cuelga o el modo suspend no se desencadena. También puede ocurrir que no se descarguen o detengan módulos o servicios que eviten el paso al modo suspend. En ambos casos se recomienda localizar el módulo defectuoso que ha impedido el modo `sleep`. Para ello pueden utilizarse los archivos de registro del daemon powersave en `/var/log/<sleep_mode>`. Si el ordenador ni siquiera pasa al modo `sleep`, la causa del problema debe buscarse en el módulo descargado en último lugar. Puede utilizar las siguientes opciones de configuración en el archivo `/etc/sysconfig/powersave/sleep` para descargar los módulos problemáticos antes de efectuar un suspend o standby.

```
POWERSAVE_UNLOAD_MODULES_BEFORE_SUSPEND2DISK=""
POWERSAVE_UNLOAD_MODULES_BEFORE_SUSPEND2RAM=""
POWERSAVE_UNLOAD_MODULES_BEFORE_STANDBY=""
POWERSAVE_SUSPEND2DISK_RESTART_SERVICES=""
POWERSAVE_SUSPEND2RAM_RESTART_SERVICES=""
POWERSAVE_STANDBY_RESTART_SERVICES=""
```

Si se utiliza suspend/standby en entornos de red cambiantes o en conexión con sistemas de archivos montados de forma remota como Samba o NIS, se recomienda montarlos con automounter o añadir los servicios correspondientes (por ejemplo `smbfs` o `nfs`) a las variables mencionadas arriba. En caso de que un programa acceda a un sistema de archivos montado de forma remota antes de iniciarse

el modo suspend/standby, el servicio no podrá detenerse correctamente ni el sistema de archivos ser compartido de forma adecuada. Después de restablecer el sistema puede que el sistema de archivos esté dañado y deba montarse de nuevo.

Powersave no percibe los límites de la batería con ACPI

En sistemas con ACPI, el sistema operativo puede pedir a la BIOS una notificación cuando se rebasa un nivel determinado de carga de la batería. La ventaja de este método es que no es necesario leer continuamente el nivel de la batería, lo que repercutiría negativamente en el rendimiento del ordenador. No obstante, puede ocurrir que, a pesar de que debería funcionar según la BIOS, esta notificación no se produzca ni siquiera al rebasar el límite.

Si observa este fenómeno en su sistema, asigne el valor `yes` a la variable `POWERSAVED_FORCE_BATTERY_POLLING` en el archivo `/etc/sysconfig/powersave/battery` para forzar la lectura del estado de la batería.

16.6. El módulo de gestión de energía de YaST

El módulo de gestión de energía de YaST le permite configurar todas las opciones relacionadas con la gestión de energía descritas en las secciones anteriores. Después de iniciar el módulo desde el centro de control de YaST con 'Sistema' → 'Gestión de energía', aparece la primera máscara del módulo (ver figura **??** en esta página).

En esta máscara puede seleccionar los perfiles o "schemes" que deben emplearse con los distintos modos de operación del sistema (con batería o conectado a la red eléctrica). Aquí puede seleccionar del menú desplegable cualquiera de los perfiles disponibles, o bien acceder a una lista de los perfiles existentes por medio del botón 'Editar perfiles'.

Seleccione en la lista el perfil que desea modificar y pulse en 'Editar'. Para crear un nuevo perfil pulse en el botón 'Añadir'. El diálogo que aparece a continuación es idéntico en ambos casos y se muestra en la figura **??** en esta página).

En primer lugar, asigne un nombre y una descripción al perfil que desea crear o modificar. A continuación defina si desea regular la potencia de la CPU para este perfil y, en caso afirmativo, cómo. Asimismo, configure las opciones 'CPU Frequency Scaling' y 'Throttling' (decida si desea utilizarlas y, en caso afirmativo,

Figura 16.1: *Selección de perfiles*

a qué nivel). En el siguiente diálogo puede definir una estrategia para el modo standby ('Standby Policy') orientada bien a conseguir un rendimiento máximo o un bajo consumo de energía. Las directrices acústicas ('Acoustic Policy') regulan el nivel de ruido del disco duro (por desgracia, sólo unos pocos discos duros IDE soportan esta opción). La sección 'Cooling Policy' regula el tipo de refrigeración que debe emplearse. Desgraciadamente, la BIOS no suele soportar este tipo de ajuste de la temperatura. En el archivo `/usr/share/doc/packages/powersave/README.thermal` se explica cómo utilizar el ventilador y los métodos pasivos de refrigeración. Una vez seleccionadas todas las opciones para el perfil, abandone este diálogo con 'Aceptar' y vuelva al diálogo de inicio. Allí puede seleccionar el perfil recién creado para uno de los dos modos de operación. La nueva configuración se activa al cerrar el diálogo con 'Aceptar'.

Además de seleccionar el perfil para los distintos modos de operación, el diálogo de inicio le ofrece también la posibilidad de configurar opciones globales para la gestión de energía, para lo que puede utilizar los botones 'Avisos de la batería', 'Configuración ACPI' o 'Activar suspend'. Pulse 'Avisos de la batería' para acceder al diálogo sobre el estado de carga de la batería (figura **??** en esta página).

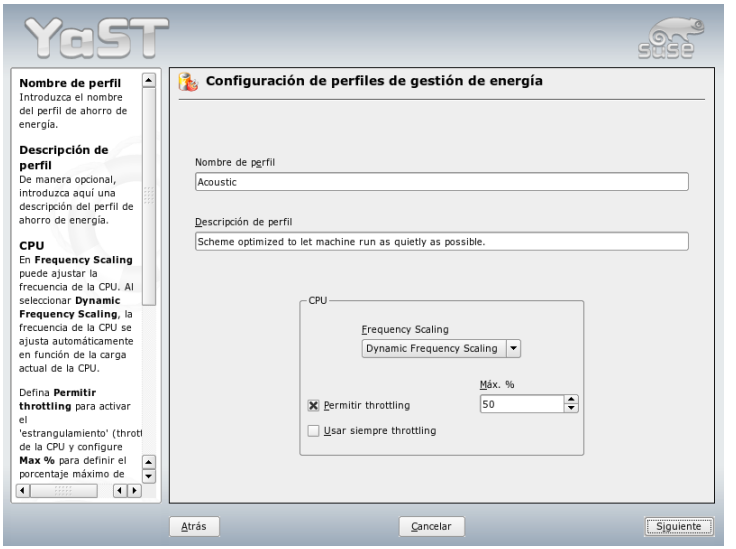

Figura 16.2: *Crear un nuevo perfil*

En cuanto se rebasa un nivel de capacidad previamente definido, la BIOS envía una notificación al sistema operativo que puede dar lugar a diversas acciones. Este diálogo le permite definir tres límites que, al ser rebasados, desencadenarán unos procesos determinados. Estos tres límites se refieren a los estados 'Aviso del nivel de batería', 'Batería baja' y 'Nivel crítico de batería'. Al alcanzar los dos primeros valores, el usuario suele recibir un mensaje de aviso. En cambio, el sobrepasar el último nivel crítico hace que el ordenador pase al modo de apagado (`shutdown`), ya que la energía restante resulta insuficiente para garantizar el funcionamiento adecuado del sistema incluso a corto plazo. Seleccione aquí los estados de carga adecuados para sus necesidades así como las acciones correspondientes. Después de abandonar el diálogo con 'Aceptar', vuelve al diálogo de inicio.

Pulse el botón 'Configuración ACPI' para acceder desde aquí al diálogo de configuración de las teclas ACPI representado en la figura **??** en esta página. Mediante la configuración de las teclas ACPI puede definir la reacción del sistema ante eventos tales como el accionamiento de un botón determinado. En ACPI se conoce a estos botones/eventos como "teclas". Aquí puede configurar la reacción del

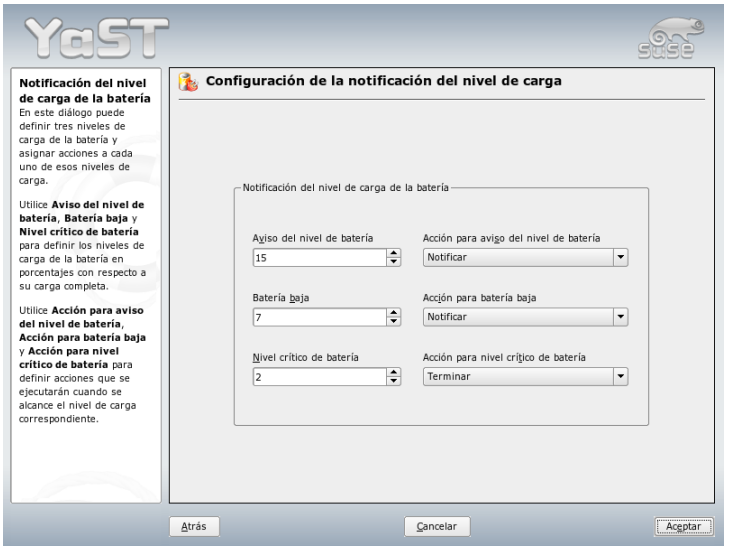

Figura 16.3: *Estado de carga de la batería*

sistema al pulsar las teclas Power, Sleep o al hecho de cerrar la tapa del portátil. Una vez definidas las opciones de configuración, pulse 'Aceptar' para salir de la máscara y volver al diálogo de inicio.

Al pulsar 'Activar suspend' aparece un diálogo en el que puede configurar si se autoriza a los usuarios del sistema a utilizar las funciones de suspend y standby y, en caso afirmativo, cómo. Pulsando de nuevo 'Aceptar', abandonará el módulo por completo y se aplicará la nueva configuración de la gestión de energía.

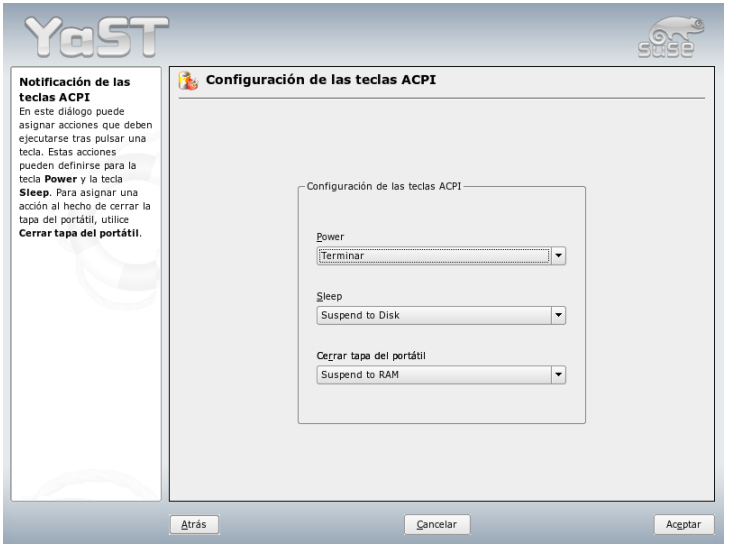

Figura 16.4: *Configuración ACPI*

Comunicación inalámbrica

Existen diversas posibilidades para comunicarse con teléfonos móviles, dispositivos periféricos y otros ordenadores desde un sistema Linux. WLAN (Wireless LAN) es la opción más adecuada para establecer una red de ordenadores portátiles. Si se trata de conectar componentes sueltos del sistema (ratón, teclado), dispositivos periféricos, teléfonos móviles, PDAs y ordenadores individuales entre sí, se recomienda emplear Bluetooth. IrDA suele utilizarse para la comunicación con PDAs o teléfonos móviles. En el presente capítulo se explican estos tres métodos así como su configuración.

17.1. LAN inalámbrica

En la actualidad, ya no podemos imaginar ningún dispositivo móvil que no pueda conectarse a las denominadas WLANs o redes inalámbricas. Hoy en día, casi ningún portátil se distribuye sin tarjeta WLAN. El estándar, según el cual las tarjetas WLAN transmiten y reciben los datos vía radio, se denomina 802.11 y fue desarrollado por el IEEE. Este estándar preveía velocidades de transmisión de hasta 2 MBit/s. No obstante, ha sido ampliado a fin de poder alcanzar mayores tasas de transmisión de datos. Estas modificaciones determinan el tipo de modulación, la potencia de transmisión y, naturalmente, las velocidades de transmisión.

Cuadro 17.1: *Resumen de los distintos estándares WLAN*

Nombre	Banda [GHz]	Tasa de transmisión máxima [MBit/s]	Observaciones
802.11	2,4	2	anticuado, prácticamente ya no existen dispositivos
802.11b	2,4	11	muy extendido
802.11a	5	54	poco extendido
802.11g	2,4	54	compatible hacia atrás con 11b

Además, existen modalidades propietarios, como por ejemplo la variante del 802.11b de Texas Instruments, con una tasa de transmisión máxima de 22 MBit/s (a veces también llamado 802.11b+). El grado de aceptación de dispositivos que utilizan esta especificación es más bien pequeño.

17.1.1. Hardware

SUSE LINUX no soporta tarjetas 802.11. En cambio, sí soporta la mayor parte de tarjetas que funcionan bajo las especificaciones 802.11a, -b y/o g. Las tarjetas actuales se basan, por lo general, en el estándar 802.11g, aunque aún existen tarjetas 802.11b. Principalmente, se soportan tarjetas con los siguientes chips:

- Lucent/Agere Hermes
- Intel PRO/Wireless 2100, 2200BG, 2915ABG
- Intersil Prism2/2.5/3
- Intersil PrismGT
- Atheros 5210, 5211, 5212
- Atmel at76c502, at76c503, at76c504, at76c506
- Texas Instruments ACX100, ACX111

También se soportan algunas tarjetas más antiguas que ya no se comercializan. Puede consultar una completa lista de tarjetas WLAN (que incluye datos como por ejemplo el chip que utilizan) en las páginas de *AbsoluteValue Systems*: `http://www.linux-wlan.org/docs/wlan_adapters.html.gz`. En la siguiente URL dispone de un resumen sobre los distintos chips WLAN: `http://wiki.uni-konstanz.de/wiki/bin/view/Wireless/ListeChipsatz`

Algunas tarjetas requieren un componente denominado Firmware-Image que debe ser cargado en la tarjeta al iniciar el controlador. Es el caso de Intersil PrismGT y Atmel ACX100, ACX111. Puede instalar el firmware fácilmente mediante la función de actualización en línea de YaST. El firmware para tarjetas PRO-Wireless de Intel está incluido en SUSE LINUX y YaST lo instala automáticamente cuando se detecta una tarjeta de este tipo. En el sistema instalado puede obtener información adicional sobre este tema en `/usr/share/doc/packages/wireless-tools/README.firmware`.

Para utilizar tarjetas sin soporte Linux nativo puede ejecutar el programa ndiswrapper. ndiswrapper emplea los controladores Windows incluidos en la mayoría de tarjetas WLAN. Puede obtener una descripción de ndiswrapper en el archivo `/usr/share/doc/packages/ndiswrapper/README.SUSE` (siempre y cuando el paquete `ndiswrapper` esté instalado). La página web del proyecto ndiswrapper (`http://ndiswrapper.sourceforge.net/support.html`) ofrece información más detallada.

17.1.2. Funcionamiento

A continuación se explican los fundamentos básicos de las redes inalámbricas, incluyendo los modos de operación y tipos de autenticación y codificación disponibles.

Modo de operación

Fundamentalmente, las redes WLAN pueden clasificarse entre redes administradas y redes ad-hoc. Las primeras poseen un componente gestionable denominado punto de acceso. Todas las conexiones de las estaciones WLAN que se encuentran en la red funcionan en este modo (también llamado modo infraestructura) a través del punto de acceso; asimismo, el punto de acceso también puede servir como elemento de conexión a una red ethernet. Las redes ad-hoc no emplean ningún punto de acceso ya que los dispositivos se comunican entre sí directamente. La cobertura y número de estaciones posibles en una red de tipo ad-hoc están fuertemente limitados, por lo que, generalmente, es preferible disponer de un punto de acceso. Existe incluso la posibilidad de que una tarjeta WLAN funcione como punto de acceso. La mayoría de tarjetas soportan esta característica.

Debido a que es más fácil acceder y controlar una red inalámbrica que una red cableada, se han previsto métodos de autentificación y cifrado para los distintos estándares. Estas especificaciones están agrupadas bajo el término WEP en la versión inicial del estándar 802.11. Como WEP ha resultado ser inseguro (véase la sección Seguridad en esta página), los fabricantes de dispositivos WLAN (agrupados en la asociación *Wi-Fi Alliance*) han definido una ampliación propia del estándar, denominada WPA, encaminada a solucionar las cuestiones de seguridad relativas a WEP. El estándar 802.11i desarrollado por el IEEE (a veces también llamado WPA2, ya que WPA era el nombre del borrador de 802.11i) comprende WPA y algunos métodos de autentificación y cifrado adicionales.

Autentificación

En las redes administradas se emplean diferentes mecanismos de autentificación para garantizar que únicamente puedan conectarse dispositivos autorizados:

Open o abierto Un sistema abierto tan sólo significa que no se lleva a cabo ninguna autentificación. Todas las estaciones están autorizadas a acceder a la red. No obstante, puede emplearse el cifrado WEP (ver sección Cifrado en esta página).

Shared Key o clave compartida (según IEEE 802.11)
Este sistema emplea la clave WEP para la autentificación. No obstante, no es recomendable utilizarlo, ya que ello implica que la clave WEP puede ser accedida con mayor facilidad. Un atacante únicamente tiene que "escuchar" la comunicación entre la estación y el punto de acceso durante una cantidad de tiempo suficiente. Durante el proceso de autentificación, ambos dispositivos intercambian la misma información, en formato cifrado y no cifrado, por lo que es posible reconstruir la clave empleada mediante

las herramientas adecuadas. Al utilizar la clave WEP tanto para la autentificación como para el cifrado, la seguridad queda comprometida. Una estación que posea la clave WEP correcta puede tanto autenticarse, como cifrar y descifrar datos. Un dispositivo que no disponga de ella, fracasará como muy tarde al descifrar los paquetes recibidos. Por lo tanto, no podrá comunicarse independientemente de que tenga o no que autentificarse.

WPA-PSK (según IEEE 802.1x) WPA-PSK (PSK para Pre Shared Key) funciona de manera parecida al procedimiento de clave compartida. Todas las estaciones participantes, así como el punto de acceso, necesitan la misma clave. La longitud de ésta es de 256 bits y se introduce normalmente como clave de acceso. Este sistema, destinado al uso privado, renuncia a una administración compleja de claves, tal y como sucede en WPA-EAP. Por tanto, a veces se identifica WPA-PSK con el término WPA "Home".

WPA-EAP (según IEEE 802.1x) En realidad, WPA-EAP no es un sistema de autentificación, sino un protocolo de autentificación para el transporte de información. Se emplea para la protección de redes inalámbricas en el sector empresarial y no tiene prácticamente ninguna presencia en el campo de las redes privadas. Por ello, se denomina a veces a WPA-EAP como WPA "Enterprise".

Cifrado

Para garantizar que ninguna persona no autorizada lea ningún paquete de datos intercambiado a través de la red inalámbrica ni pueda acceder a ésta, se utilizan los siguientes métodos de cifrado:

WEP (definido en IEEE 802.11) Este estándar utiliza al algoritmo de cifrado RC4, que inicialmente ofrecía una longitud de clave de 40 bits y que más tarde fue extendido hasta los 104 bits. A menudo, también se emplea una longitud de 64 ó 128 bits, dependiendo de si se cuentan o no los 24 bits del llamado vector de inicialización. No obstante, este estándar presenta debilidades, ya que se han constatado algunas vulnerabilidades. A pesar de esto, es preferible el empleo de WEP que ningún sistema de cifrado.

TKIP (definido en WPA/IEEE 802.11i)
Este protocolo para la admnistración de claves, definido en el estándar WPA, emplea el mismo algoritmo de cifrado que WEP, pero eliminando sus debilidades. Como se genera una nueva clave para cada paquete, los ataques contra esa clave son prácticamente inútiles. TKIP se utiliza conjuntamente con WPA-PSK.

CCMP (definido en IEEE 802.11i) CCMP, definido en IEEE 802.11i, especifica la administración de claves. Ésta se emplea normalmente conjuntamente con WPA-EAP, aunque también puede utilizarse en conjunto con WPA-PSK. El cifrado se lleva a cabo mediante AES, resultando más seguro que el cifrado RC4 del estándar WEP.

17.1.3. Configuración con YaST

Para configurar su tarjeta de red inalámbrica, inicie el módulo YaST 'Tarjeta de red'. En el diálogo 'Configuración de la dirección de red', seleccione el tipo de dispositivo 'inalámbrico' y pulse 'Siguiente'.

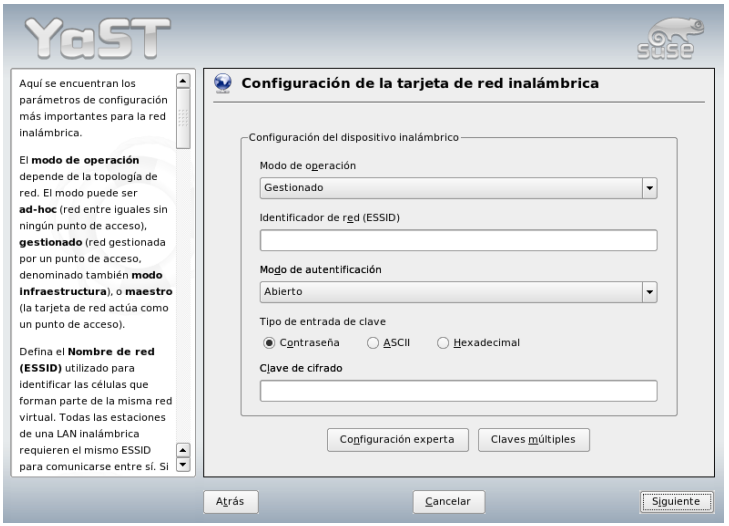

Figura 17.1: *YaST Configuración de la tarjeta de red inalámbrica*

En la ventana de diálogo 'Configuración de la tarjeta de red inalámbrica' representada en la figura **??** en esta página puede definir la configuración básica para WLAN:

Modo de operación Una estación de trabajo puede integrarse en una WLAN de tres modos distintos. El modo adecuado depende del formato de la red

a través de la cual desea comunicarse: 'ad-hoc' (red punto-a-punto pura sin punto de acceso), 'gestionado' (la red es administrada por un punto de acceso) y 'maestro' (su tarjeta de red funciona como punto de acceso).

Identificador de red (ESSID) Todas las estaciones dentro de una red inalámbrica necesitan el mismo ESSID para poder comunicarse entre ellas. En caso de que no esté predeterminado, la tarjeta busca automáticamente un punto de acceso, el cual no tiene por qué coincidir con el que pretendía utilizar inicialmente.

Modo de autentificación Elija un método de autentificación adecuado para su red. Puede escoger entre: 'abierto', 'clave compartida' y 'WPA-PSK'. Si elige 'WPA-PSK', tendrá que definir un nombre de red.

Avanzado A través de este botón puede acceder a un cuadro de diálogo de configuración avanzada WLAN. Más adelante encontrará una descripción detallada acerca de éste.

Una vez finalizada la configuración básica, su estación estará preparada para poder conectarse a la WLAN.

Importante

Seguridad en una red inalámbrica

Utilice siempre uno de los procedimientos de autentificación y cifrado soportados para proteger el tráfico de su red. Las conexiones WLAN no cifradas permiten que terceros puedan llegar a escuchar de forma ininterrumpida todos los datos transmitidos a través de la red. Incluso un cifrado débil (WEP) es mejor que ninguno. Consulte la sección Cifrado en esta página y sección Seguridad en esta página para obtener información adicional.

Importante

Dependiendo del método de autentificación elegido, YaST le solicitará que efectúe una configuración más o menos detallada. En 'Abierto' no es necesario configurar nada más, ya que esta opción establece un funcionamiento sin cifrado ni autentificación.

Claves WEP Seleccione el tipo de entrada de clave entre 'Contraseña', 'ASCII' o 'Hexadecimal' e introduzca la clave de cifrado. Puede mantener hasta

cuatro claves distintas para codificar los datos transmitidos. Pulse el botón 'Claves múltiples' para acceder al diálogo de configuración de las claves. A continuación determine la longitud de la clave: '128 bits' o '64 bits'. La configuración predeterminada es '128 bits'. En la lista inferior es posible especificar hasta cuatro claves de cifrado para la estación de trabajo. Determine qué clave utilizará habitualmente mediante la opción 'Definir como predeterminada'. La primera clave introducida es considerada por YaST como la clave estándar. Si borra la clave estándar, tendrá que seleccionar manualmente una de las claves restantes como estándar. Con 'Editar' puede modificar las entradas de la lista o crear una nueva clave. En este caso, se le solicitará que elija una de estas tres alternativas, ('Contraseña', 'ASCII' o 'Hexadecimal'). En caso de escoger 'Contraseña', introduzca una palabra o cadena de caracteres. El sistema utilizará ésta para generar una clave de longitud igual a la fijada anteriormente. 'ASCII' requiere la introducción de cinco caracteres para una longitud de clave de 64 bits y de trece caracteres en el caso de un cifrado de 128 bits. Si elige la opción 'Hexadecimal', especifique diez caracteres en notación hexadecimal en el caso de una longitud de clave de 64 bits o veintiseis para 128 bits.

WPA-PSK En el caso de una clave WPA-PSK, elija como método de entrada la opción 'Contraseña' o 'Hexadecimal'. En modo 'Contraseña', la cadena introducida ha de comprender entre ocho y sesenta y tres caracteres; en modo 'Hexadecimal' serán necesarios sesenta y cuatro caracteres.

Mediante 'Avanzado' podrá acceder a la configuración avanzada desde el cuadro diálogo de configuración básica. En él, se encuentran disponibles las siguientes opciones:

Canal Sólo es necesario el establecimiento de un canal en los modos 'ad-hoc' o 'maestro'. Bajo la modalidad 'gestionado', la tarjeta examina automáticamente los canales disponibles en busca de puntos de acceso. En modo 'ad-hoc' puede seleccionar uno de los 12 canales que se muestran. Si el formato seleccionado es 'maestro', tendrá que determinar cuál es el canal que va a emplear la tarjeta para realizar la función de punto de acceso. La configuración predeterminada de esta opción es 'auto'.

Tasa de bits Dependiendo de la eficiencia de su red, puede que sea conveniente predeterminar una velocidad de transferencia concreta con la que transmitir datos desde un punto a otro. La opción 'auto' intentará transmitir los datos a la mayor velocidad posible. Tenga en cuenta que no todas las tarjetas WLAN permiten establecer la velocidad de transmisión.

Punto de acceso Si la red dispone de varios puntos de acceso, podrá seleccionar uno en particular introduciendo su dirección MAC.

Usar gestión de energía Si se encuentra lejos de una toma de corriente, es recomendable que optimice duración de la batería mediante el uso de técnicas de ahorro de energía. Puede obtener más información acerca de la administración de energía bajo Linux en el capítulo ?? en esta página.

17.1.4. Programas útiles

hostap (paquete `hostap`) se emplea para poder utilizar una tarjeta WLAN como punto de acceso. Puede obtener una amplia información acerca de este paquete en la página principal del proyecto (`http://hostap.epitest.fi/`).

kismet (paquete `kismet`) es una herramienta para el diagnóstico de redes con la que podrá escuchar o monitorizar el tráfico de paquetes dentro de la WLAN y, asimismo, localizar posibles intentos de intrusión en la red. Puede obtener más información en `http://www.kismetwireless.net/` o en su página man.

17.1.5. Consejos y trucos para configurar una WLAN

A continuación se describe cómo ajustar la velocidad y estabilidad de la WLAN y se mencionan algunos aspectos de seguridad.

Estabilidad y velocidad

El hecho de que una red inalámbrica funcione de manera eficiente y fiable depende principalmente de si los dispositivos participantes reciben una señal limpia de los demás. Los obstáculos, como paredes, atenúan la señal de forma sensible. La velocidad de transmisión también disminuye considerablemente si la señal se debilita. En KDE puede determinar la potencia de la señal por medio del programa iwconfig desde la línea de comandos (apartado `Link Quality`) o mediante kwifimanager. En caso de que tenga problemas con la calidad de la señal, intente instalar los equipos siguiendo otra disposición o modificar la orientación de la antena de su punto de acceso. Existen antenas accesorias para algunas tarjetas PCMCIA WLAN que mejoran notablemente la recepción. La velocidad declarada por el fabricante (por ejemplo, 54 MBit/s) es siempre un valor nominal. Además, se trata del máximo teórico. En la práctica, la velocidad máxima de transmisión real suele ser la mitad de este valor.

Seguridad

Durante el despliegue de una red inalámbrica, ha de tener en cuenta que si no implanta medidas de seguridad adicionales, cualquiera que se encuentre dentro de su cobertura podrá acceder fácilmente a ella. Por tanto, debería configurar siempre algún método de cifrado. Todos los dispositivos inalámbricos, sea una tarjeta WLAN o un punto de acceso, soportan el formato de cifrado incluido en el protocolo WEP. Éste no es absolutamente seguro, pero representa un obstáculo para un atacante potencial. Por tanto, normalmente, WEP es suficiente para el uso privado. Sería aún mejor emplear WPA-PSK, pero éste no está implementado en los routers o puntos de acceso más antiguos que ofrecen funcionalidades WLAN. Algunos pueden soportar WPA si se actualiza el firmware, otros no. Linux tampoco soporta WPA bajo todos los dispositivos de hardware. En estos momentos, WPA funciona sólo con tarjetas que utilicen un chip Atheros o Prism2/2.5/3. Con este último, ha de instalarse el controlador hostap (véase la sección Problemas con tarjetas Prism2 en esta página). Si no es posible emplear WPA, se recomienda utilizar el nivel anterior: WEP es siempre mejor que ningún cifrado. En el entorno empresarial, en el que se suelen establecer requisitos de seguridad más exigentes que en el doméstico, sólo debería utilizarse WPA.

17.1.6. Posibles problemas y sus soluciones

En caso de que su tarjeta WLAN no funcione correctamente, asegúrese en primer lugar de que dispone de la versión de firmware necesaria. Puede obtener más información en la sección **??** en esta página. En ella se incluyen también algunos consejos para otros problemas frecuentes.

Múltiples dispositivos de red

Los portátiles actuales disponen normalmente de una tarjeta de red y de una tarjeta WLAN. En caso de que haya configurado ambos equipos con DHCP (asignación automática de direcciones IP), es posible que experimente problemas con la resolución de nombres y la pasarela. Es posible que éste sea el caso si no puede navegar por Internet, pero sí puede hacer un ping al router. Puede encontrar información adicional acerca de este tema buscando "DHCP" en `http://portal.suse.de/sdb/de/index.html`.

Problemas con tarjetas Prism2

Existen varios controladores disponibles para dispositivos basados en los chips Prism2. Con estas tarjetas, WPA sólo está disponible si se utiliza el controla-

dor hostap. En caso de que esté experimentando algún problema con alguna de estas tarjetas (si no funciona o lo hace sólo esporádicamente) o si desea emplear WPA, consulte el archivo `/usr/share/doc/packages/wireless-tools/README.prism2`.

WPA

El soporte para WPA ha sido implementado recientemente en SUSE LINUX y, en general, aún no está muy desarrollado en Linux. Mediante YaST, sólo puede configurarse WPA-PSK. WPA no funciona con muchas tarjetas y algunas necesitan una actualización del firmware antes de poder emplear WPA. Si desea utilizar WPA, le recomendamos que consulte el archivo `/usr/share/doc/packages/wireless-tools/README.wpa`.

17.1.7. Información adicional

Puede obtener abundante información acerca de redes inalámbricas en la página web de Jean Tourrilhes, autor de las aplicaciones *Wireless Tools* para Linux: `http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html`

17.2. Bluetooth

Bluetooth es una tecnología de radio que permite conectar distintos dispositivos, teléfonos móviles, PDAs, dispositivos periféricos o componentes del sistema como el teclado o el ratón y portátiles entre sí. El nombre tiene su origen en el rey danés Harold Blatand (en inglés "Harold Bluetooth"), que vivió en el siglo X en la región escandinava y logró unificar diversas fracciones enfrentadas. El logotipo de Bluetooth se basa en las runas de sus iniciales: "H" (semejante a una estrella) y "B".

Bluetooth se diferencia de IrDA en algunos aspectos importantes: por una parte, los distintos dispositivos no deben "verse" necesariamente; por otra, varios dispositivos pueden agruparse y formar redes completas. No obstante, actualmente sólo pueden alcanzarse tasas de datos de hasta 720 Kbps como máximo (al menos en la versión actual 1.2). En teoría, con Bluetooth es posible establecer conexiones entre dispositivos separados por una pared. En la práctica, esto depende en gran medida de la pared y de la clase de dispositivo. Esta última determina el alcance máximo de la transmisión, que varía de diez a cien metros dependiendo de cuál de las tres clases se utilice.

17.2.1. Fundamentos

A continuación se describe a grandes rasgos el funcionamiento de Bluetooth, explicando temas como los requisitos de software, la interacción de Bluetooth con el sistema y el funcionamiento de los perfiles Bluetooth.

Software

Para poder utilizar Bluetooth es necesario contar con un adaptador Bluetooth (integrado en el dispositivo o bien como llave de hardware externa o dongle), controladores y la pila de protocolo para Bluetooth ("Bluetooth Protocol Stack"). El kernel de Linux contiene ya los controladores básicos para el uso de Bluetooth. En cuanto a la pila de protocolo se utiliza el sistema Bluez. Asimismo, los paquetes básicos `bluez-libs` y `bluez-utils` deben estar instalados para que las distintas aplicaciones funcionen con Bluetooth. Dichos paquetes proporcionan servicios o programas de servicio que el sistema necesita. Para algunos adaptadores (Broadcom, AVM BlueFritz!) se requiere además el paquete `bluez-firmware`. El paquete `bluez-cups` posibilita la impresión a través de conexiones Bluetooth.

Interacción general

Los sistemas Bluetooth están formados por cuatro capas interdependientes, cada una de las cuales cumple una función determinada:

Hardware El adaptador y un controlador adecuado que garantiza el soporte en el kernel Linux.

Archivos de configuración El control del sistema Bluetooth.

Daemons Servicios que proporcionan diversas funciones y que están controlados a través de los archivos de configuración.

Aplicaciones Programas que ponen al alcance del usuario las funciones proporcionadas por los daemons y que les permiten controlar dichas funciones.

Al conectar un adaptador Bluetooth, el controlador correspondiente se carga a través del sistema hotplug. Una vez que el controlador está cargado, se comprueba por medio de los archivos de configuración si Bluetooth debe iniciarse. En caso afirmativo, se determina qué servicios han de iniciarse y, en función de estos, se activan los daemons correspondientes. El sistema comprueba la existencia de

adaptadores Bluetooth durante la instalación. Si se encuentra uno o varios, Bluetooth es activado. En caso contrario, el sistema Bluetooth se desactiva. Si se añade algún dispositivo Bluetooth con posterioridad, debe ser activado manualmente.

Perfiles

Los servicios en Bluetooth se definen por medio de perfiles. Así por ejemplo, en la versión estándar de Bluetooth existen perfiles para la transferencia de archivos (perfil "File Transfer"), la impresión (perfil "Basic Printing") y las conexiones en red (perfil "Personal Area Network").

Para que un dispositivo pueda utilizar un servicio de otro, ambos deben entender el mismo perfil. Desgraciadamente, ni la documentación ni la caja del dispositivo incluyen con frecuencia esta información. Otra dificultad añadida es que algunos fabricantes respetan escrupulosamente la definición de cada perfil y otros no. A pesar de ello, en la práctica los dispositivos consiguen "entenderse" por regla general.

En el texto siguiente, los dispositivos locales son aquellos conectados físicamente al ordenador. Los dispositivos a los que sólo puede accederse a través de conexiones inalámbricas se denominarán en adelante dispositivos remotos.

17.2.2. Configuración

A continuación se describe la configuración de Bluetooth. Entre los temas tratados cabe destacar los archivos de configuración relevantes, las herramientas de configuración necesarias y la posibilidad de configurar Bluetooth manualmente o con YaST.

Configuración de Bluetooth con YaST

El módulo Bluetooth de YaST (ver figura **??** en esta página) le permite configurar el soporte Bluetooth. Tan pronto como hotplug detecta un adaptador Bluetooth en el sistema (por ejemplo durante el arranque o al conectarlo), Bluetooth se inicia con la configuración definida en este módulo.

En el primer paso de la configuración puede definir si los servicios Bluetooth han de iniciarse en el sistema. Si ya ha activado los servicios Bluetooth puede configurar dos cosas. En primer lugar el 'Nombre de dispositivo', que es el nombre mostrado por otros dispositivos cuando el ordenador es detectado. Para introducirlo puede utilizar dos comodines: `%h`, que sustituye al nombre de máquina (útil en los casos en los que este se asigne dinámicamente por DHCP) y `%d`, que

Figura 17.2: *YaST: configuración de Bluetooth*

sustituye al nombre de interfaz (de utilidad sólo si dispone de varios adaptadores Bluetooth en la máquina). Por ejemplo, si introduce en la casilla el nombre `Laptop%h` y DHCP asigna a la máquina el nombre `unit123`, otros dispositivos remotos mostrarán el equipo como `Laptop unit123`.

El segundo parámetro, 'Administrador de seguridad', afecta al comportamiento del sistema local cuando un dispositivo remoto intenta conectarse con el mismo. La diferencia radica en el uso del PIN. Existen varias posibilidades: permitir a cualquier dispositivo la conexión sin PIN o, en caso de que el PIN sea necesario, determinar cómo se elige. Puede introducir un PIN (guardado en un archivo de configuración) en la casilla de texto disponible a tal efecto. Cuando un dispositivo intente conectarse, utilizará primero este PIN. Si el mecanismo falla, se aplica la opción sin PIN. El nivel más alto de seguridad lo proporciona la tercera opción "Pedir siempre el PIN al usuario". Esta le permite utilizar distintos PINS para dispositivos (remotos) diferentes.

Pulse el botón 'Configuración avanzada del daemon' para acceder al diálogo de selección y configuración detallada de los servicios ofrecidos (o *perfiles*, como se denominan en Bluetooth). En el diálogo se muestra una lista de todos los servi-

cios disponibles, los cuales puede activar o desactivar con los botones 'Activar' o 'Desactivar'. Pulsando 'Editar' se activa una ventana emergente en la que es posible asignar distintos argumentos al servicio (daemon) seleccionado. Modifique las opciones predeterminadas sólo si conoce bien el servicio en cuestión. Después de configurar el daemon, salga de este diálogo con 'OK'.

De vuelta en el diálogo principal, pulse el botón 'Opciones de seguridad' para acceder al diálogo de seguridad. En él puede definir, entre otras, la configuración relacionada con la criptografía así como los métodos de autenticación y de sondeo. Una vez definida la configuración de seguridad, regresará al diálogo principal. Cuando salga de este diálogo con 'Finalizar', el sistema Bluetooth estará listo para el uso.

Desde el diálogo principal también es posible acceder a la ventana de 'Clases de dispositivos y servicios'. Los dispositivos Bluetooth se dividen en varias "Clases de dispositivo". En este diálogo puede escoger la que corresponda a su equipo como "equipo de sobremesa" o "portátil". La clase de dispositivo no es muy importante a diferencia de la "Clase de servicio", que también se define aquí. En ocasiones, los dispositivos Bluetooh remotos como los teléfonos móviles sólo permiten algunas funciones si en el sistema se ha detectado la clase de servicio adecuada. Este suele ser el caso de teléfonos móviles que esperan una clase llamada "Transferencia de objetos" antes de permitir la transferencia de archivos desde o hacia el ordenador. Aunque puede elegir varias clases, no se recomienda elegirlas todas "por si acaso". La selección predeterminada resultará adecuada casi siempre.

Si desea utilizar Bluetooth para establecer una red, active el 'PAND' en el diálogo 'Configuración avanzada del daemon' y utilice la opción 'Editar' para definir el modo del daemon. Para que la conexión de red Bluetooth funcione, pand debe operar en el modo de escucha ('listen') y el conector en el de búsqueda (modo 'search'). El modo predeterminado es el de escucha. Si es necesario, ajuste el modo del pand local. Asimismo, utilice el módulo de YaST 'Tarjetas de red' para configurar la interfaz `bnepX` (`X` representa el número de dispositivo en el sistema).

Configuración manual de Bluetooth

Los archivos de configuración para los distintos componentes del sistema Bluez se recogen en el directorio `/etc/bluetooth`. La única excepción la constituye el archivo utilizado para iniciar los componentes, `/etc/sysconfig/bluetooth`, el cual es procesado por el módulo de YaST.

Los archivos de configuración que se describen a continuación sólo pueden ser modificados por `root`. Actualmente no existe ninguna interfaz gráfica para configurar *todos* los parámetros. Los más importantes pueden definirse mediante el

módulo Bluetooth de YaST que se describe en la sección Configuración de Bluetooth con YaST en esta página. Las demás opciones de configuración sólo son relevantes para usuarios experimentados con necesidades específicas. Para el resto, las opciones predeterminadas serán suficientes en la mayoría de los casos.

Un número de identificación personal (PIN) constituye la primera medida de protección frente a conexiones no deseadas. Los teléfonos móviles suelen preguntar este PIN en el primer contacto (o al configurar en el teléfono el contacto con el dispositivo). Para que dos dispositivos puedan comunicarse entre sí, ambos deben identificarse con el mismo PIN. Este se encuentra almacenado en el ordenador en el archivo `/etc/bluetooth/pin`.

Importante

Seguridad en las conexiones Bluetooth

El uso de PINs no garantiza que la conexión entre dos dispositivos esté libre de escuchas por parte de terceros. Tenga presente que tanto la autenticación como la codificación de conexiones Bluetooth están desactivadas en la configuración predeterminada. Al activar ambas opciones puede ocurrir que se produzcan problemas en la comunicación con algunos dispositivos Bluetooth.

Importante

En el archivo de configuración `/etc/bluetooth/hcid.conf` es posible modificar algunas opciones de configuración tales como nombres de dispositivos y modos de seguridad. Los valores predeterminados de las opciones de configuración resultarán adecuados en casi todas las ocasiones. El archivo incluye comentarios que describen los parámetros posibles en las distintas opciones. Aquí nos limitaremos a mencionar dos de ellas.

El archivo contiene dos secciones llamadas `options` y `device`. La primera incluye información de carácter general que es utilizada por hcid durante el inicio. La segunda contiene opciones de configuración para cada uno de los dispositivos Bluetooth locales.

Una de las principales opciones de configuración de la sección `options` es `security auto;`. Si se le ha asignado el valor `auto`, hcid intenta usar el PIN local para las conexiones entrantes. Si este proceso falla, usa el valor predeterminado `Ninguno` y establece la conexión de todos modos. Para mantener un cierto nivel de seguridad se recomienda cambiar el valor predeterminado a `user` para que en cada conexión se le pida al usuario el PIN.

En la sección `device` se puede especificar el nombre con el que el ordenador será mostrado en el otro extremo de la conexión. También se define la clase de disposi-

tivo (`sobremesa`, `portátil`, `servidor`, etc.) y se activa o desactiva la autenticación y la codificación.

17.2.3. Componentes del sistema y herramientas

El uso de Bluetooth sólo es posible gracias a la combinación de varios servicios. Como mínimo es necesario que dos daemons se estén ejecutando en segundo plano: hcid (*Host Controller Interface*), el cual actúa de interfaz con el dispositivo Bluetooth y lo controla, y sdpd (*Service Discovery Protocol*), que informa a un dispositivo remoto de los servicios que ofrece el ordenador. Tanto hcid como sdpd pueden iniciarse — en caso de que no haya sucedido automáticamente al arrancar el sistema — con el comando `rcbluetooth start`, que debe ser ejecutado como usuario `root`.

A continuación se describen las principales herramientas shell que pueden utilizarse para trabajar con Bluetooth. Aunque ya existen diversos componentes gráficos para manejar Bluetooth, se recomienda echar un vistazo a estos programas.

Algunos comandos sólo pueden ejecutarse como usuario `root`, como por ejemplo `l2ping` ⟨*dirección_dispositivo*⟩, con el que se puede probar la conexión a un dispositivo remoto.

hcitool

Por medio de hcitool es posible averiguar si se han encontrado dispositivos locales y/o remotos. El comando `hcitool dev` muestra el propio dispositivo. Para cada dispositivo encontrado localmente se muestra una línea con la siguiente estructura: ⟨*nombre_interfaz*⟩ ⟨*dirección_dispositivo*⟩.

Para detectar dispositivos remotos puede utilizarse el comando `hcitool inq`. La salida de este comando muestra tres valores por cada dispositivo encontrado: la dirección y la clase de dispositivo y una diferencia horaria. El valor más importante es la dirección de dispositivo, que es usada por otros comandos para identificar el dispositivo destino. La diferencia horaria es sólo interesante desde el punto de vista técnico. En cuanto a la clase de dispositivo, en ella se recoge el tipo de dispositivo y de servicio en forma de valor hexadecimal.

Con `hcitool name` ⟨*dirección_dispositivo*⟩ se puede averiguar el nombre de un dispositivo remoto. Si se trata por ejemplo de otro ordenador, la clase y nombre de dispositivo mostrados deben coincidir con la información recogida en el archivo `/etc/bluetooth/hcid.conf` de este ordenador. Las direcciones de dispositivos locales generan un mensaje de error.

hciconfig

`/usr/sbin/hciconfig` proporciona información adicional sobre el dispositivo local. Al ejecutar `hciconfig` sin argumentos se muestran datos del dispositivo como su nombre (`hciX`), la dirección física de dispositivo (un número de 12 cifras con el formato `00:12:34:56:78`) e información sobre la cantidad de datos transmitidos.

`hciconfig hci0 name` muestra el nombre con el que el ordenador responde a solicitudes de dispositivos remotos. `hciconfig` no sólo sirve para ver la configuración del dispositivo local sino también para modificarla. Por ejemplo, el comando `hciconfig hci0 name TEST` cambia el nombre a `TEST`.

sdptool

El programa sdptool proporciona información sobre los servicios ofrecidos por un dispositivo determinado. El comando `sdptool browse` ⟨*`dirección_dispositivo`*⟩ muestra todos los servicios de un dispositivo, mientras que `sdptool search` ⟨*`abreviatura_servicio`*⟩ permite buscar un servicio concreto. Este comando pregunta a todos los dispositivos disponibles por el servicio deseado. Si este es ofrecido por alguno de los dispositivos, el programa proporciona al usuario el nombre completo del servicio ofrecido por el dispositivo junto con una breve descripción del mismo. Al ejecutar `sdptool` sin ningún parámetro se muestra una lista de todas las abreviaturas de servicios posibles.

17.2.4. Aplicaciones gráficas

Al introducir la URL `bluetooth:/`, Konqueror muestra los dispositivos Bluetooth locales y remotos. Pulsando dos veces con el ratón sobre un dispositivo aparece una lista con los servicios ofrecidos por el mismo. Cuando se mueve el ratón sobre uno de los servicios, se muestra en la ventana de estado de la parte inferior del navegador el perfil utilizado para dicho servicio. Al pulsar sobre un servicio se abre una ventana en la que puede elegir diversas acciones: guardar, utilizar el servicio (para ello debe iniciarse una aplicación) o cancelar la acción. Aquí también puede definir que la ventana no vuelva a mostrarse y que siempre se ejecute la acción seleccionada. Tenga en cuenta que algunos servicios (todavía) no están soportados y que para otros puede ser necesario añadir algunos paquetes.

17.2.5. Ejemplos

A continuación se presentan dos ejemplos típicos de posibles escenarios Bluetooth. El primero ilustra una conexión Bluetooth entre dos ordenadores y el segundo entre un ordenador y un teléfono móvil.

Conexión de red entre dos ordenadores C1 y C2

En el primer ejemplo se va a establecer una conexión de red entre dos ordenadores *C1* y *C2*. Las direcciones de dispositivo Bluetooth de estos ordenadores son *baddr1* y *baddr2*. Estas direcciones pueden averiguarse en ambos ordenadores con la ayuda del comando `hcitool dev` como se ha descrito arriba. Al final del proceso, los ordenadores han de poder verse con la dirección IP `192.168.1.3` (*C1*) y `192.168.1.4` (*C2*).

La conexión Bluetooth se establece por medio del programa pand (personal area networking). Los siguientes comandos deben ser ejecutados por `root`. La siguiente descripción se concentra en las acciones específicas de Bluetooth y no ofrece una explicación detallada del comando de red `ip`.

Introduzca el comando `pand -s` para iniciar pand en *C1*. A continuación puede establecer una conexión en *C2* introduciendo el comando `pand -c` ⟨*baddr1*⟩. Si ejecuta el comando `ip link show` en una de las máquinas para ver la lista de interfaces de red disponibles, obtendrá una entrada como la siguiente:

```
 bnep0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
link/ether 00:12:34:56:89:90 brd ff:ff:ff:ff:ff:ff
```

En lugar de `00:12:34:56:89:90` aparecerá la dirección local del dispositivo *baddr1* o bien *baddr2*. Ahora es necesario asignar una dirección IP a esta interfaz y seguidamente activarla. Para ello se ejecutan por ejemplo los siguientes comandos en *C1*:

```
ip addr add 192.168.1.3/24 dev bnep0
ip link set bnep0 up
```

o de forma análoga en *C2*

```
ip addr add 192.168.1.4/24 dev bnep0
ip link set bnep0 up
```

Ya es posible acceder a *C1* desde *C2* con la dirección IP `192.168.1.3`. El comando `ssh 192.168.1.4` le permite acceder a *C2* desde *C1* (siempre que sshd esté ejecutándose en *C2*, como es el caso en la configuración estándar de SUSE LINUX). El comando `ssh 192.168.1.4` también puede ejecutarse como usuario "normal".

Transmisión de datos desde un teléfono móvil al ordenador

En el segundo ejemplo, vamos a transmitir una imagen creada con un teléfono móvil con cámara a un ordenador sin incurrir en gastos adicionales como sería por ejemplo el envío de un mensaje multimedia. Tenga en cuenta que cada teléfono móvil dispone de una estructura de menús diferente, pero el proceso será parecido en casi todos ellos. En caso necesario, consulte las instrucciones del teléfono. A continuación se describe la transmisión de una fotografía desde un teléfono Sony Ericsson a un ordenador portátil. Para ello es necesario que el servicio Obex-Push esté disponible en el ordenador y que el ordenador permita el acceso del teléfono móvil. En el primer paso se activará el servicio en el portátil. Esto se realiza con el daemon opd incluido en el paquete `bluez-utils`. Para iniciar este daemon, ejecute el comando:

```
opd --mode OBEX --channel 10 --daemonize --path /tmp --sdp
```

En este comando merece la pena destacar dos parámetros: el parámetro `--sdp` registra el servicio en sdpd y `--path /tmp` comunica al programa dónde debe almacenar los datos recibidos (en este caso en `/tmp`). Aquí también es posible introducir otras rutas. Para ello sólo necesita permiso de escritura en el directorio especificado.

A continuación, el teléfono debe "conocer" al ordenador. Con este fin, busque en el teléfono el menú 'Conexiones' y seleccione la entrada 'Bluetooth'. Si es necesario, pulse 'Activar' antes de escoger el punto 'Dispositivos propios'. Seleccione 'Nuevo dispositivo' y espere a que el teléfono encuentre el portátil. Cuando se encuentra un dispositivo, este se muestra con su nombre en la pantalla del móvil. Seleccione el dispositivo que corresponda al portátil. A continuación se le preguntará por el PIN (aquí debe introducir el PIN que aparece en `/etc/bluetooth/pin`). Una vez introducido el PIN correcto, el teléfono y el portátil se "conocen" y pueden intercambiar datos. Salga del menú y pase al menú de fotografías. Seleccione la imagen que desea transmitir y pulse la tecla 'Más'. Pulsando 'Enviar' en el menú que aparece a continuación, podrá elegir la forma de envío: seleccione 'Bluetooth'. Ahora debería poder definir el portátil como dispositivo destino. Tras efectuar esta selección, la fotografía es transmitida

al portátil y guardada en el directorio especificado al ejecutar opd. Este procedimiento también puede emplearse para trasmitir otro tipo de datos, como por ejemplo un archivo de música.

17.2.6. Posibles problemas y sus soluciones

En caso de problemas de conexión se recomienda comprobar los siguientes puntos. No obstante, tenga siempre presente que el problema puede residir en cualquiera de los extremos de la conexión o, en el peor de los casos, en ambos. Si es posible, reconstruya el problema con un dispositivo Bluetooth distinto para excluir así fallos en el dispositivo:

¿Aparece el dispositivo local en la salida de `hcitool dev`?
Si el dispositivo local no aparece en la salida de este comando, es posible que hcid no se haya iniciado o que el dispositivo no sea detectado como dispositivo Bluetooth. Esto puede obedecer a distintas causas, como que el dispositivo esté estropeado o falte el controlador adecuado. En el caso de portátiles con Bluetooth incorporado suele haber un interruptor para dispositivos operados por radio como WLAN y Bluetooth. Consulte en la documentación del fabricante si el portátil dispone de un interruptor de este tipo. Reinicie el sistema Bluetooth con `rcbluetooth restart` y examine el archivo `/var/log/messages` para ver si hay mensajes de error.

¿Necesita el adaptador Bluetooth un archivo Firmware?
En este caso instale `bluez-bluefw` y reinicie el sistema Bluetooth con `rcbluetooth restart`.

¿Aparecen en la salida de `hcitool inq` otros dispositivos?
En este caso vuelva a probar de nuevo; puede que hubiera algún problema con la conexión la primera vez. La banda de frecuencia de Bluetooth es utilizada también por otros dispositivos.

¿Coinciden los PINs? Compruebe si el PIN en `/etc/bluetooth/pin` y el PIN del dispositivo destino coinciden.

¿El otro dispositivo puede "ver" su ordenador?
Intente iniciar la conexión desde otro dispositivo y compruebe si el nuevo dispositivo "ve" al ordenador.

¿Es posible establecer una conexión de red (ejemplo 1)?

Si el primer ejemplo (conexión de red) no funciona puede deberse a distintas causas. Por ejemplo, puede ser que uno de los dos ordenadores no entienda el protocolo ssh. Pruebe a ejecutar el comando `ping 192.168.1.3` o `ping 192.168.1.4`. En caso de obtener respuesta, compruebe si sshd está activo. Otra posible causa es que ya disponga de otras direcciones que entren en conflicto con las direcciones utilizadas en el ejemplo `192.168.1.X`. Repita el proceso con otras direcciones, como por ejemplo `10.123.1.2` y `10.123.1.3`.

¿Aparece el portátil como dispositivo destino (ejemplo 2)? ¿Detecta el teléfono móvil el servicio Obex-Push en el portátil?

Vaya al menú 'Dispositivos propios', seleccione el dispositivo correspondiente y consulte la 'Lista de servicios'. Si en ella no aparece Obex-Push (aún después de actualizar la lista), la causa del problema es opd en el portátil. ¿Se ha iniciado opd? ¿Tiene permiso de escritura en el directorio especificado?

¿Funciona el segundo ejemplo también a la inversa?

Si ha instalado el paquete `obexftp`, la transmisión de datos funciona en algunos teléfonos con el comando `obexftp -b` ⟨*`dirección_dispositivo`*⟩ `-B 10 -p` ⟨*`nombre_imagen`*⟩. Se han probado distintos modelos de las marcas Siemens y Sony Ericsson y funcionan. Vea a este respecto la documentación del paquete en `/usr/share/doc/packages/obexftp`.

17.2.7. Información adicional

Puede encontrar una amplia lista de documentación relacionada con el funcionamiento y la configuración de Bluetooth en: `http://www.holtmann.org/linux/bluetooth/`. Otras fuentes de información útiles:

- Conexión con PDAs PalmOS: `http://www.cs.ucl.ac.uk/staff/s.zachariadis/btpalmlinux.html`
- HOWTO oficial del *Bluetooth Protocol Stack* integrado en el kernel: `http://bluez.sourceforge.net/howto/index.html`

17.3. Transmisión de datos por infrarrojos

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, modems, 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 controlador especial para el chip IrDA, pero no existen controladores para todos los chips. Además se debe configurar el modo deseado en el setup de la BIOS. Allí se puede averiguar también la conexión serie 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/`.

17.3.1. 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. Una vez instalado el paquete, la documentación al respecto se encuentra en `/usr/share/doc/packages/irda/README`.

17.3.2. Configuración

IrDA no se inicia automáticamente al arrancar, sino que debe activarse con el módulo IrDA de YaST. En este módulo sólo se puede modificar una opción de configuración: la interfaz serie del dispositivo infrarrojo. La ventana de prueba está dividida en dos partes. En la parte superior se muestra la salida de `irdadump` donde se registran todos los paquetes IrDA enviados y recibidos. En esta salida debe aparecer regularmente el nombre del ordenador y el nombre de todos los dispositivos infrarrojos en el radio de acción. Puede ver un ejemplo de esta salida de comando en la sección **??** en esta página. En la parte inferior de la pantalla se muestran todos los dispositivos con los que existe una conexión IrDA.

Desgraciadamente, IrDA requiere bastante energía (corriente externa o batería), puesto que envía un paquete Discovery cada dos segundos con el fin de detectar

automáticamente otros dispositivos periféricos. Así pues, si trabaja con batería se recomienda arrancar IrDA sólo cuando lo vaya a utilizar. Puede activar manualmente la conexión con el comando `rcirda start` y desactivarla con `rcirda stop`. Al activar la conexión se cargarán automáticamente los módulos del kernel necesarios.

La configuración manual se lleva a cabo en el archivo `/etc/sysconfig/irda`. Allí sólo hay una variable, `IRDA_PORT`, que determina qué interfaz se va a utilizar en modo SIR.

17.3.3. Uso

Para imprimir por vía infrarroja, es posible enviar los datos a través del archivo de dispositivo `/dev/irlpt0`. Este se comporta igual que la interfaz o archivo de dispositivo `/dev/lp0` con conexión por cable, sólo que los datos viajan por vía infrarroja. A la hora de imprimir, asegúrese de que la impresora se encuentra a la vista de la interfaz infrarroja del ordenador y de que el soporte infrarrojo está activado.

Una impresora que trabaja con el puerto IrDA puede configurarse con YaST del modo acostumbrado. Como no será detectada automáticamente, seleccione la categoría 'Otro (no detectado)'. En el siguiente diálogo puede elegir la opción 'Impresora IrDA'. Como conexión se puede utilizar casi siempre `irlpt0`. Para obtener información adicional sobre la impresión en Linux, consulte el capítulo ?? en esta página.

El archivo 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 sincronizar datos con el PDA Palm Pilot, para lo cual sólo tiene que introducir `/dev/ircomm0` como dispositivo en el programa correspondiente.

Sólo es posible comunicarse directamente con dispositivos que soportan los protocolos Printer o IrCOMM. Los programas especiales irobexpalm3 o irobexreceive también permiten establecer comunicación con dispositivos que utilizan el protocolo IROBEX (3Com Palm Pilot). Consulte el *IR-HOWTO* (`http://tldp.org/HOWTO/Infrared-HOWTO/`) para más información. Los protocolos soportados por el dispositivo aparecen entre corchetes en la salida de `irdadump` después del nombre de dispositivo. El soporte del protocolo IrLAN aún se encuentra en desarrollo ("work in progress").

17.3.4. Posibles problemas y sus soluciones

Si los dispositivos en el puerto de infrarrojos no reaccionan, se puede comprobar si el ordenador detecta el otro dispositivo ejecutando el comando `irdadump` como usuario `root`. Si hay una impresora Canon BJC-80 a la vista del ordenador, aparece el siguiente mensaje en la pantalla, repitiéndose periódicamente (ver ejemplo **??** en esta página).

Ejemplo 17.1: *Salida de irdadump*

```
21:41:38.435239 xid:cmd 5b62bed5 > ffffffff S=6 s=0 (14)
21:41:38.525167 xid:cmd 5b62bed5 > ffffffff S=6 s=1 (14)
21:41:38.615159 xid:cmd 5b62bed5 > ffffffff S=6 s=2 (14)
21:41:38.705178 xid:cmd 5b62bed5 > ffffffff S=6 s=3 (14)
21:41:38.795198 xid:cmd 5b62bed5 > ffffffff S=6 s=4 (14)
21:41:38.885163 xid:cmd 5b62bed5 > ffffffff S=6 s=5 (14)
21:41:38.965133 xid:rsp 5b62bed5 < 6cac38dc S=6 s=5 BJC-80
                        hint=8804 [Printer IrCOMM ] (23)
21:41:38.975176 xid:cmd 5b62bed5 > ffffffff S=6 s=* tierra
                        hint=0500 [ PnP Computer ] (21)
```

Si no aparece nada en pantalla o el otro dispositivo no responde, debe comprobar primero la configuración de la interfaz. ¿Está usando la interfaz correcta? La interfaz infrarroja se encuentra a veces también en `/dev/ttyS2` o `/dev/ttyS3`. Igualmente, 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; a diferencia de los ojos humanos, la mayoría de las cámaras de vídeo pueden ver la luz infrarroja.

El sistema hotplug

El sistema hotplug regula el inicio de la mayoría de dispositivos de un ordenador. No sólo afecta a los dispositivos que pueden conectarse y desconectarse mientras el sistema está activo, sino también a aquellos detectados durante el arranque del sistemas. El sistema hotplug colabora estrechamente con el sistema de archivos `sysfs` y `udev`, los cuales se describen en el capítulo **??** en esta página.

Antes del arranque del kernel, sólo se inician dispositivos imprescindibles como pueden ser el bus, los disquetes de arranque o el teclado. El kernel desencadena eventos hotplug para todos los dispositivos detectados. El daemon `udevd` escucha dichos eventos y activa los scripts hotplug correspondientes para iniciar esos dispositivos. Para dispositivos que no pueden detectarse automáticamente o cuyos eventos se ha perdido al iniciarse el arranque, existe el sistema coldplug. Este sistema reproduce eventos guardados o busca en el sistema dispositivos sin iniciar y utiliza configuraciones estáticas para dispositivos antiguos como por ejemplo ISA.

Actualmente, la mayoría de dispositivos (excepto algunas excepciones por razones históricas) son iniciados en cuanto es posible acceder a ellos, bien durante el arranque o al ser conectados. Durante el inicio, las interfaces se registran en el kernel. Este regristro a su vez desencadena varios eventos hotplug que hacen que la interfaz se configure automáticamente.

En antiguas versiones de SUSE LINUX se partía de un conjunto estático de datos de configuración que, al aplicarse, causaba el inicio de dispositivos. Hoy en día, el sistema examina los dispositivos disponibles y busca para ellos datos de configuración adecuados o bien los genera.

Existen dos archivos para la configuración de las funciones hotplug más importantes. `/etc/sysconfig/hotplug` alberga variables para modificar el comportamiento de `hotplug` y `coldplug`. El archivo contiene comentarios que explican el significado de cada variable. El archivo `/proc/sys/kernel/hotplug` muestra el nombre del programa que ejecuta el kernel para realizar el soporte hotplug. La configuración de los dispositivos se encuentra en el archivo `/etc/sysconfig/hardware`. Desde la distribución SUSE LINUX 9.3, este archivo suele estar vacío ya que `udevd` recibe los mensajes hotplug a través de un socket netlink.

18.1. Dispositivos e interfaces

El sistema hotplug gestiona interfaces además de dispositivos. Un dispositivo (*device*) siempre está conectado a una interfaz o a un bus. Un bus puede considerarse como una interfaz múltiple. Una interfaz (*interface*) conecta dispositivos entre sí o a una aplicación. Además de dispositivos físicos existen también dispositivos virtuales (por ejemplo un túnel de red). Los dispositivos necesitan normalmente controladores en forma de módulos del kernel. Las interfaces suelen estar representadas por nodos de dispositivo creados por `udev`. La distinción entre dispositivo e interfaz es fundamental para entender el concepto completo.

Los dispositivos registrados en el sistema de archivos `sysfs` se encuentran en `/sys/devices` mientras que las interfaces están en `/sys/class` o `/sys/block`. Todas las interfaces incluidas en `sysfs` deberían contar con un enlace (*link*) a su dispositivo. No obstante, todavía existen algunos controladores que no añaden este enlace automáticamente. Sin este enlace no es posible determinar a qué dispositivo pertenece una interfaz ni encontrar una configuración adecuada.

Se accede a los dispositivos a través de una descripción de dispositivo. Esta descripción puede ser el "devicepath" en `sysfs` (`/sys/devices/pci0000:00/0000:00:1e.0/0000:02:00.0`), una descripción del lugar de conexión (`bus-pci-0000:02:00.0`), un ID individual (`id-32311AE03FB82538`) o una descripción similar. Hasta ahora, para acceder a una interfaz siempre se utilizaba su nombre. Estos nombres eran simplemente una numeración correlativa de los dispositivos disponibles y podían cambiar al añadir o eliminar dispositivos.

También es posible acceder a una interfaz por medio de la descripción del dispositivo respectivo. Según el contexto, en cada caso se distingue si la descripción se refiere al dispositivo o a su interfaz. A continuación se presentan algunos ejemplos típicos de dispositivos, interfaces y descripciones:

Tarjeta de red PCI Es un dispositivo conectado al bus PCI (`/sys/devices/pci0000:00/0000:00:1e.0/0000:02:00.0` o bien `bus-pci-0000:02:00.0`) que dispone de una interfaz de red (`eth0`, `id-00:0d:60:7f:0b:22` o bien `bus-pci-0000:02:00.0`). Esta interfaz es utilizada por servicios de red o está conectada a un dispositivo de red virtual como un túnel o VLAN que a su vez posee una interfaz.

Controladora SCSI PCI Es un dispositivo (`/sys/devices/pci0000:20/0000:20:01.1/host1/1:0:0:0` o `bus-scsi-1:0:0:0`) que ofrece varias interfaces físicas en forma de un bus (`/sys/class/scsi_host/host1`).

Disco duro SCSI Un dispositivo (`/sys/devices/pci0000:20/0000:20:01.1/host1/1:0:0:0` o `bus-scsi-1:0:0:0`) con varias interfaces (`/sys/block/sda*`).

18.2. Eventos hotplug

Existe un evento hotplug específico para cada dispositivo y cada interfaz. Estos eventos son procesados por `udev` y el agente hotplug correspondiente. El kernel

desencadena un evento hotplug cuando se crea o elimina un enlace a un dispositivo o cuando un controlador registra o borra una interfaz. Desde SUSE LINUX 9.3, `udevd` recibe y emite eventos hotplug. Para ello, `udevd` escucha directamente los mensajes netlink del kernel o bien `/sbin/udevsend` debe especificarse en `/proc/sys/kernel/hotplug`. Después de completar su trabajo (ver capítulo **??** en esta página), `udevd` busca en `/etc/hotplug.d/` un agente hotplug acorde con el tipo de evento.

18.3. Agentes hotplug

Un agente hotplug es un programa ejecutable que se encarga de llevar a cabo las acciones adecuadas para un evento. Los agentes para los eventos de dispositivo se encuentran en `/etc/hotplug.d/`⟨*nombre_evento*⟩ y `/etc/hotplug.d/default`. Todos los programas con la extensión `.hotplug` que se encuentran en estos directorios son ejecutados en orden alfabético.

Para lograr que los eventos de un determinado tipo sean ignorados, elimine los bits ejecutables de los agentes hotplug respectivos. Otro método consiste en cambiar `.hotplug` a cualquier otra cosa.

Aunque los agentes de dispositivos cargan normalmente módulos del kernel, en ocasiones deben ejecutar otros comandos. En SUSE LINUX son `/sbin/hwup` y `/sbin/hwdown` los que se encargan de ello. Estos dos programas buscan en el directorio `/etc/sysconfig/hardware` una configuración adecuada para el dispositivo y la aplican. En caso de que un dispositivo concreto no deba iniciarse, se creará un archivo de configuración apropiado con el modo de inicio `manual` u `off`. Si `/sbin/hwup` no encuentra ninguna configuración, el agente carga los módulos automáticamente. En este caso, algunos agentes general de manera automática archivos de configuración para `hwup`. Esto hace que el agente se ejecute más rápido la próxima vez. Puede obtener información adicional en la sección **??** en esta página. Dispone de más información sobre `/sbin/hwup` en el archivo `/usr/share/doc/packages/sysconfig/README` y en la página del manual de `man hwup`.

Antes de que se activen los agentes de interfaz, `udev` suele generar un enlace de dispositivo (*device node*) al que puede acceder el sistema. `udev` ofrece la posibilidad de asignar nombres permanentes a las interfaces. Puede obtener más información al respecto en el capítulo ?? en esta página. Finalmente, cada agente se encarga de configurar las interfaces. A continuación se describe este procedimiento para algunas interfaces.

18.3.1. Activación de interfaces de red

Las interfaces de red se activan con `/sbin/ifup` y se desactivan con `/sbin/ifdown`. Para obtener información adicional, consulte el archivo `/usr/share/doc/packages/sysconfig/README` y la página man `man ifup`.

En caso de que un ordenador disponga de varios dispositivos de red con controladores distintos, puede ocurrir que el nombre de una interfaz se modifique si otro controlador se carga más rápidamente durante el arranque. Por este motivo, los eventos para dispositivos de red PCI se administran en SUSE LINUX por medio de una cola. Puede desactivar este comportamiento en el archivo `/etc/sysconfig/hotplug` por medio de la variable `HOTPLUG_PCI_QUEUE_NIC_EVENTS=no`.

La mejor solución consiste en utilizar nombres de interfaz permanentes. Para ello debe introducir los nombres de cada interfaz en los archivos de configuración. El archivo `/usr/share/doc/packages/sysconfig/README` contiene información adicional sobre este método. Aunque no sean nodos de dispositivo, desde SUSE LINUX 9.3, `udev` también se encarga de las interfaces de red. Esto permite el uso de nombres permanentes de interfaces de forma más estandarizada.

18.3.2. Activación de dispositivos de almacenamiento

Para poder acceder a los a los dispositivos de almacenamiento, es necesario conectar interfaces a los mismos. Este proceso puede automatizarse o preconfigurarse completamente. La configuración se realiza en las variables `HOTPLUG_DO_MOUNT`, `HOTPLUG_MOUNT_TYPE` y `HOTPLUG_MOUNT_SYNC` del archivo `/etc/sysconfig/hotplug` y en el archivo `/etc/fstab`. Para activar el proceso automatizado, defina la variable `HOTPLUG_DO_MOUNT=yes`. Si desea desactivar el proceso, asígnele el valor `no`

La operación automática soporta dos modos, subfs o fstab, entre los que puede alternarse por medio de la variable `HOTPLUG_MOUNT_TYPE`.

En el modo `HOTPLUG_MOUNT_TYPE=subfs`, se crea en el directorio `/media` un subdirectorio cuyo nombre se deriva de las características del dispositivo. Al acceder al medio de almacenamiento, este se monta y desmonta automáticamente en este subdirectorio por medio de `submountd`. Los datos se escriben inmediatamente, por lo que en este modo los dispositivos pueden retirarse simplemente cuando dejan de ser accesibles. En el modo `HOTPLUG_MOUNT_TYPE=fstab`, los dispositivos de almacenamiento se montan por medio de una entrada en el archivo `/etc/fstab` según el método tradicional.

Con la variable HOTPLUG_MOUNT_SYNC se puede especificar si el acceso tiene lugar en modo síncrono o asíncrono. En el modo asíncrono el acceso de escritura es mucho más rápido ya que los resultados se guardan en la memoria intermedia; no obstante, es posible que los datos no puedan escribirse completamente si el medio de almacenamiento no es retirado correctamente. En el modo síncrono todos los datos se escriben de forma inmediata, por lo que el acceso es algo más lento. El dispositivo debe desmontarse manualmente con umount.

Se recomienda utilizar nombres de dispositivo persistentes en lugar de nombres tradicionales, que pueden modificarse dependiendo del orden de inicio. Puede obtener información adicional sobre los nombres de dispositivo persistentes en el capítulo ?? en esta página.

18.4. Carga automática de módulos

Si no ha sido posible iniciar un dispositivo utilizando /sbin/hwup, el agente busca un controlador adecuado dentro de los "module maps". Primero se busca en los mapas de /etc/hotplug/*.handmap y, si la búsqueda no tiene éxito, también en /lib/modules/<versión_kernel>/modules.*map. Para utilizar otro controlador que no sea el controlador estándar del kernel debe introducirlo en el archivo /etc/hotplug/*.handmap, que es el que se evalúa en primer lugar.

En USB y PCI existen algunas particularidades. El agente USB busca también controladores de modo usuario en los archivos /etc/hotplug/usb.usermap y /etc/hotplug/usb/*.usermap. Se denomina controladores de modo usuario a aquellos que no regulan un módulo del kernel sino el acceso a un dispositivo. De este modo también es posible activar otros programas ejecutables para dispositivos determinados.

En el caso de los dispositivos PCI, pci.agent busca primero los controladores con hwinfo. Si hwinfo no encuentra ningún controlador, el agente consulta pci.handmap y kernelmap. Esto ya lo ha hecho hwinfo previamente, con lo cual el segundo intento no funcionará tampoco. hwinfo dispone de una base de datos adicional para las correspondencias de controladores. No obstante, también carga el archivo pci.handmap para garantizar la aplicación de correspondencias individuales que puedan haberse definido en este archivo.

Se puede reducir la búsqueda de controladores del agente pci.agent a dispositivos de un tipo concreto o a determinados subdirectorios de /lib/modules/<versión_kernel>/kernel/drivers. En el primer caso, es posible introducir clases de dispositivo PCI tal y como aparecen al final del archivo

/usr/share/pci.ids en las variables HOTPLUG_PCI_CLASSES_WHITELIST y HOTPLUG_PCI_CLASSES_BLACKLIST del archivo /etc/sysconfig/hotplug. En el segundo caso, el/los directorios deseados se han de especificar en el archivo /etc/sysconfig/hotplug utilizando las variables HOTPLUG_PCI_DRIVERTYPE_WHITELIST o HOTPLUG_PCI_DRIVERTYPE_BLACKLIST. Los módulos de los directorios excluidos nunca se cargan. En ambos casos, si la "whitelist" permanece vacía, significa que todas las posibilidades son válidas excepto las excluidas en la lista negra. También es posible excluir módulos individuales del proceso de carga. Para ello introduzca en el archivo /etc/hotplug/blacklist los módulos que no deban ser cargados bajo ningún concepto. Cada nombre de módulo se introduce en una línea aparte.

Si se encuentran varios módulos adecuados dentro de un archivo map, sólo se carga el primero. Para cargar todos los módulos, se define la variable HOTPLUG_LOAD_MULTIPLE_MODULES=yes. No obstante, es mejor todavía crear una configuración propia para este dispositivo: /etc/sysconfig/hardware/hwcfg-*.

Esto no se refiere a los módulos que se cargan con el comando hwup. La carga automática de módulos está reducida a casos excepcionales que serán aún más raros en las futuras ediciones de SUSE LINUX. No obstante, si se ha encontrado un módulo adecuado, el agente crea un archivo de configuración hwup que se usará la próxima vez. De esta forma se incrementa la velocidad de inicio del dispositivo.

18.5. Hotplug con PCI

Ciertos ordenadores permiten el cambio en caliente de dispositivos PCI. Para poder utilizar esta función en todo su alcance es necesario cargar módulos especiales de kernel que pueden provocar problemas en ordenadores que no dispongan de soporte hotplug para PCI. Dado que no se puede detectar automáticamente las ranuras PCI con capacidad de hotplug, esta función ha de configurarse manualmente. Asigne para ello el valor yes a la variable HOTPLUG_DO_REAL_PCI_HOTPLUG en el archivo /etc/sysconfig/hotplug.

18.6. El script de arranque coldplug

boot.coldplug se ocupa de todos los dispositivos que no han sido detectados automáticamente; es decir, de aquellos para los que no se genera ningún evento

hotplug. En este caso simplemente se activa `hwup` para cada configuración estática de dispositivo `/etc/sysconfig/hardware/hwcfg-static-*`. También puede emplearse para iniciar los dispositivos integrados en un orden distinto al que utilizaría hotplug, ya que `coldplug` se ejecuta antes que `hotplug`.

18.7. Análisis de fallos

18.7.1. Archivos de registro

En su configuración predeterminada, `hotplug` envía sólo unos pocos mensajes a `syslog`. Para ampliar la información de registro, asigne el valor `yes` a la variable `HOTPLUG_DEBUG` en el archivo `/etc/sysconfig/hotplug`. Si el valor asignado es `max`, se registran todos los comandos shell de todos los scripts de hotplug y el archivo `/var/log/messages`, utilizado por `syslog` para guardar los mensajes, crece en consecuencia. Al arrancar el ordenador, `syslog` se inicia después de `hotplug` y `coldplug`, por lo que los primeros mensajes no se guardan. Si estos fueran importantes, se utiliza otro archivo de registro modificando la variable `HOTPLUG_SYSLOG`. Consultar también los comentarios en `/etc/sysconfig/hotplug`.

18.7.2. Problemas de arranque

Si el ordenador se queda colgado durante el arranque, desactive `hotplug` o `coldplug` introduciendo en el prompt de arranque `NOHOTPLUG=yes` o bien `NOCOLDPLUG=yes`. Al desactivar hotplug el kernel deja de producir eventos hotplug. Cuando el sistema esté activo puede volver a activar hotplug con el comando `/etc/init.d/boot.hotplug start`. Al activarlo se emiten y procesan todos los eventos generados hasta ese momento. Para desechar los eventos retenidos, puede introducir previamente `/bin/true` en `/proc/sys/kernel/hotplug` y, pasado un tiempo, volver a activar `/sbin/hotplug`. La desactivación de coldplug sólo tiene como efecto la no aplicación de la configuración estática. Puede volver a activarlo en cualquier momento con `/etc/init.d/boot.coldplug start`.

Para averiguar si un módulo cargado por `hotplug` es la causa del problema, introduzca `HOTPLUG_TRACE=<N>` en el prompt de arranque. Ahora el ordenador espera $\langle N \rangle$ segundos antes de cargar los módulos y muestra los nombres de los mismos en pantalla. No se puede intervenir en este proceso.

18.7.3. La grabadora de eventos

El script `/sbin/hotplugeventrecorder` se ejecuta con cualquier evento de `/sbin/hotplug`. Si existe un directorio `/events`, todos los eventos hotplug se guardan como archivos sueltos en este directorio. De esta forma es posible volver a crear cualquier evento con fines de pruebas. Los eventos sólo se guardan si existe este directorio.

Nodos de dispositivos dinámicos con udev

El kernel 2.6 de Linux ofrece una solución nueva en el espacio de usuario (*user space*) para un directorio de dispositivos dinámico `/dev` con denominaciones permanentes de dispositivos: `udev`. `udev` sólo proporciona archivos para los dispositivos realmente presentes. Crea o elimina archivos de nodos de dispositivos que normalmente se encuentran en el directorio `/dev` y cambia el nombre de las interfaces de red. La implementación anterior de `/dev` con `devfs` ya no funciona y ha sido sustituida por `udev`.

Tradicionalmente, en los sistemas Linux se grababan enlaces de dispositivos (*device nodes*) en el directorio `/dev`. Existía un enlace para cualquier tipo posible de dispositivo, independientemente de su existencia real en el sistema. Como consecuencia, el directorio `/dev` resultante podía llegar a ser muy grande. La introducción de `devfs` supuso una mejora sustancial, ya que sólo los dispositivos realmente existentes contaban con un nodo de dispositivo en `/dev`.

`udev` se sirve de un método nuevo para crear los nodos de dispositivos: compara la información recibida por `sysfs` con las reglas definidas por el usuario. `sysfs` es un sistema de archivos nuevo incorporado en el kernel 2.6 que ofrece información básica sobre los dispositivos conectados al sistema. `sysfs` está montado en `/sys`.

La definición de reglas por parte del usuario no es imprescindible. En cuanto un dispositivo se conecta, se crea también el enlace correspondiente. La reglas ofrecen la posibilidad de cambiar los nombres de los enlaces, lo que permite reemplazar los nombres crípticos de dispositivo por otros más fáciles de recordar. Además es posible tener nombres permanentes de dispositivo cuando se conectan dos dispositivos del mismo tipo.

Dos impresoras conectadas al sistema reciben por defecto la denominación `/dev/lp0` y `/dev/lp1`. No obstante, la asignación de nombres (qué impresora recibe qué nodo de dispositivo) depende del orden en el que se encienden. Otro ejemplo son los dispositivos de almacenamiento externos tales como los discos duros USB. `udev` permite definir rutas exactas de dispositivo en `/etc/fstab`.

19.1. Fundamentos de la creación de reglas

Antes de crear enlaces a dispositivos en `/dev`, `udev` evalúa todos los archivos en `/etc/udev/rules.d` con la extensión `.rules` en orden alfabético. La primera regla que puede aplicarse a un dispositivo es la que se utiliza, independientemente de que haya reglas adicionales que también puedan aplicarse. Los comentarios comienzan con el símbolo #. Las reglas tienen la forma:

```
Clave, [clave,...] NAME [, SYMLINK]
```

Se precisa por lo menos una clave que se encargue de asignar la regla a un dispositivo. El nombre es igualmente imprescindible porque se utiliza para crear el

enlace al dispositivo en /dev. El parámetro opcional para enlaces simbólicos permite la creación de enlaces en otros lugares. Una regla para una impresora puede tener el siguiente aspecto:

```
BUS="usb", SYSFS{serial}="12345", NAME="lp_hp", SYMLINK="printers/hp"
```

Este ejemplo tiene dos claves: BUS y SYSFS{serial}. udev compara el número de serie indicado con el número de serie del dispositivo conectado al bus USB. Todas las claves deben ser iguales para que se asigne el nombre lp_hp al dispositivo en el directorio /dev. Además se crea un enlace simbólico llamado /dev/printers/hp que apunta al enlace de dispositivo. Al mismo tiempo, el directorio printers se crea automáticamente. Las tareas de impresión se pueden mandar indistintamente a /dev/printers/hp o a /dev/lp_hp.

19.2. Automatización con NAME y SYMLINK

Los parámetros NAME y SYMLINK permiten el uso de parámetros para automatizar una asignación determinada de nombres y dispositivos. Los parámetros se refieren a datos del kernel sobre un cierto dispositivo. El siguiente ejemplo muestra esta función:

```
BUS="usb", SYSFS{vendor}="abc", SYSFS{model}="xyz", NAME="camera%n"
```

El parámetro %n en el nombre se sustituye por el número de dispositivo de la cámara: camera0, camera1, etc. Otro parámetro útil es %k, que representa el nombre de dispositivo estándar del kernel como por ejemplo hda1. También es posible activar un programa externo en las reglas udev y utilizar la secuencia devuelta en los valores NAME y SYMLINK. La página del manual de udev muestra una lista de todos los parámetros.

19.3. Expresiones regulares en claves

Es posible utilizar comodines como expresiones regulares dentro de las claves. De igual manera que en la shell, se puede emplear, por ejemplo, el carácter * como comodín para cualquier cadena de caracteres o ? para un carácter cualquiera.

```
KERNEL="ts*", NAME="input/%k"
```

Esta regla hace que un dispositivo cuya denominación comienza con las letras "ts", reciba el nombre del kernel estándar en el directorio predeterminado. Para obtener información detallada sobre el uso de expresiones regulares en las reglas udev, consulte la página del manual `man udev`.

19.4. Selección de claves adecuadas

Para que una regla udev funcione correctamente ha de haberse seleccionado una clave correcta. Claves típicas son, por ejemplo:

BUS Tipo de bus del dispositivo.

KERNEL Nombre de dispositivo usado por el kernel.

ID Número de dispositivo en el bus (ej. ID del bus PCI).

PLACE Lugar físico de conexión del dispositivo (ej. USB).

SYSFS{...} Atributos de dispositivo sysfs como el nombre, fabricante, número de serie, etc.

Aunque las claves ID y Place pueden resultar muy útiles, las más utilizadas son BUS, KERNEL y SYSFS{...}. Además, `udev` ofrece claves que ejecutan scripts externos y evalúan los resultados de los mismos. Puede obtener información adicional al respecto en la página del manual `man udev`.

`sysfs` crea en el árbol de directorios unos archivos pequeños con información sobre el hardware. Cada archivo no contiene más información que el nombre de dispositivo, el fabricante o el número de serie. Cada uno de estos archivos puede utilizarse como valor para la clave. Si desea utilizar varias claves SYSFS{...} en una sola regla, sólo puede emplear archivos del mismo directorio como valores de clave. Puede utilizar la herramienta `udevinfo` para encontrar valores de clave adecuados.

En `/sys` debe encontrar un subdirectorio que se refiera al dispositivo correspondiente y contenga un archivo `dev`. Los directorios con estas características se encuentran en `/sys/block` o `/sys/class`. Si ya existe un nodo para el

dispositivo, `udevinfo` puede encontrar el subdirectorio adecuado. El comando `udevinfo -q path -n /dev/sda` devuelve `/block/sda`, lo que significa que el directorio requerido es `/sys/block/sda`. A continuación active `udevinfo` con el comando `udevinfo -a -p /sys/block/sda`. También es posible combinar los dos comandos de la forma `udevinfo -a -p 'udevinfo -q path -n /dev/sda'`. A continuación se muestra un extracto de la salida de este comando:

```
BUS="scsi"
ID="0:0:0:0"
SYSFS{detach_state}="0"
SYSFS{type}="0"
SYSFS{max_sectors}="240"
SYSFS{device_blocked}="0"
SYSFS{queue_depth}="1"
SYSFS{scsi_level}="3"
SYSFS{vendor}="        "
SYSFS{model}="USB 2.0M DSC    "
SYSFS{rev}="1.00"
SYSFS{online}="1"
```

Busque en las indicaciones claves adecuadas e invariables y recuerde que no es posible utilizar claves de diferentes directorios dentro de una misma regla.

19.5. Nombres permanentes de dispositivo

SUSE LINUX incorpora varios scripts que le permiten asignar siempre los mismos nombres de dispositivo a discos duros y otros dispositivos de almacenamiento independientemente del orden en que se inicien. Por ejemplo, el script de envoltorio (wrapper-script) `/sbin/udev.get_persistent_device_name.sh` activa primero a `/sbin/udev.get_unique_hardware_path.sh`, que se encarga de averiguar la ruta a un dispositivo determinado. `/sbin/udev.get_unique_drive_id.sh` consulta el número de serie. `udev` recibe el resultado de ambos comandos y crea enlaces simbólicos al nodo de dispositivo en `/dev`. Es posible utilizar el wrapper-script directamente dentro de las reglas udev. Abajo figura un ejemplo para SCSI que también puede utilizarse en USB e IDE (todo debe introducirse en una sola línea):

```
BUS="scsi",
PROGRAM="/sbin/udev.get_persistent_device_name.sh",
NAME="%k" SYMLINK="%c{1+}"
```

Cuando se carga un controlador para un dispositivo de almacenamiento, registra todos los discos duros existentes con el kernel. Cada disco genera un evento de hotplug que activa `udev`. `udev` lee primero la reglas para averiguar si se debe crear un enlace simbólico.

Los eventos hotplug se pierden si el controlador se carga a través de `initrd`. Sin embargo, toda la información relevante queda guardada en `sysfs`. La herramienta `udevstart` encuentra todos los archivos de dispositivo en `/sys/block` y `/sys/class` antes de iniciar `udev`.

Existe un script de inicio adicional llamado `boot.udev`. Durante el arranque, este script se encarga de crear de nuevo todos los nodos de dispositivo. Es preciso activar el script utilizando el editor de niveles de ejecución de YaST o por medio del comando `insserv boot.udev`.

Sugerencia

Existen diversos programas y herramientas cuyo correcto funcionamiento depende de que encuentren un disco duro de tipo SCSI en `/dev/sda` y un disco duro IDE en `/dev/hda`. Puesto que YaST necesita estas herramientas, utiliza sólo las denominaciones de dispositivo del kernel.

Sugerencia

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 ofrece información sobre el soporte de archivos grandes o "Large File Support".

20.1. Glosario

Metadatos Estructura interna de los datos de un sistema de archivos que garantiza el orden de la estructura y la disponibilidad de los datos del 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 causa de las diferencias en cuanto a rendimiento de los sistemas de archivos. Es extremadamente importante mantener intactos los metadatos, ya que de lo contrario se podría dañar todo el sistema de archivos.

Inode Los inodes contienen toda la información sobre un archivo: el nombre, el tamaño, el número de enlaces, la fecha, la hora en que fue creado, modificaciones, accesos como "señalador" (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.

20.2. 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 pueda 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 ”coherencia de los datos” no se refieren en este capítulo a la coherencia de los datos que un usuario tiene guardados (los datos que una aplicación escribe en los archivos). La coherencia de estos datos debe quedar asegurada por las aplicaciones mismas.

Importante

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.

Importante

20.2.1. ReiserFS

Aunque oficialmente se trata de una de las prestaciones principales de la versión 2.4 del kernel, ReiserFS ha estado disponible desde la versión 6.4 de SUSE LINUX como parche para el kernel de SUSE 2.2.x. ReiserFS es producto de la labor 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 rendimiento optimizado del acceso al disco y una recuperación más rápida después de una caída del sistema. A continuación se describen con detalle las principales ventajas de ReiserFS:

Las principales ventajas de ReiserFS son:

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 del B*tree (árbol), en lugar de guardarlos en otro lugar y luego tener que administrar el puntero (pointer) para que apunte al sitio indicado. Además, la memoria no se asignará en unidades de 1 a 4 Kb, sino en la unidad exactamente 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 densidad del inode en el momento de crear el sistema de archivos.

Mejor rendimiento del acceso al disco duro
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.

Fiabilidad gracias al registro de datos (data journaling)
ReiserFS también soporta el registro de datos y los modos "ordered" de datos (ambos conceptos se explican con más detalle en la sección **??** en esta página). El modo predeterminado es `data=ordered`, lo que garantiza la integridad tanto de los datos como de los metadatos. No obstante, el registro se utiliza sólo para los metadatos.

20.2.2. 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 hecho ganarse la reputación de ser "sólido como una roca". 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 lleva 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 complementarían perfectamente con las ventajas de los sistemas de archivos journaling.

20.2.3. 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 sencilla 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 por ejemplo 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 se tiene que desmontar el sistema Ext3 y montarlo como Ext2.

Fiabilidad y rendimiento Otros sistemas de archivos journaling siguen el principio journaling de "sólo metadatos" (metadata-only). Esto significa que

los metadatos permanecen en un estado coherente, lo que sin embargo no puede garantizarse 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 (es decir, 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 de datos se escriben en el disco antes de que los metadatos sean actualizados. Con esto se consigue la coherencia 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 mientras se garantiza la integridad del sistema de archivos. Mientras no se indique otra opción, Ext3 arrancará con la opción predeterminada `data=ordered`.

20.2.4. Conversión de un sistema de archivos Ext2 a Ext3

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 los parámetros `size=` y `device=`. Puede obtener información adicional sobre tune2fs en las páginas del manual.

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.

Uso de Ext3 para el sistema de archivos raíz
Para arrancar el sistema de archivos raíz (`root`) en `ext3`, hace falta integrar adicionalmente los módulos `ext3` y `jbd` en el RAM disk inicial `initrd`. A continuación introduzca estos dos módulos en el archivo `/etc/sysconfig/kernel` bajo `INITRD_MODULES`. Posteriormente ejecute el comando `mk_initrd`.

20.2.5. Reiser4

Inmediatamente después de que el kernel 2.6 viera la luz, un nuevo miembro se sumó a la familia de sistemas de archivos transaccionales: Reiser4. Reiser4 se diferencia sustancialmente de su predecesor ReiserFS (versión 3.6). Introduce el concepto de plugins para configurar las funciones del sistema de archivos y un concepto de seguridad más elaborado.

Concepto de seguridad muy elaborado
Durante el diseño de Reiser4, los desarrolladores pusieron especial énfasis en la implementación de funciones relacionadas con la seguridad. Como consecuencia, Reiser4 incorpora un conjunto de plugins de seguridad dedicados, el más importante de los cuales introduce el concepto de elementos de archivo o "items". Actualmente, el control de acceso a los archivos se define en función del archivo. Si existe un archivo muy grande que contiene información relevante para varios usuarios, grupos o aplicaciones, los permisos de acceso deben ser poco precisos para incluir a todos los interesados. En Reiser4 es posible dividir este tipo de archivos en porciones más pequeñas ("items"). Los permisos de acceso pueden definirse para cada elemento y usuario, permitiendo una gestión de seguridad de archivos mucho más precisa. El archivo `/etc/passwd` constituye un ejemplo perfecto. Actualmente, `root` es el único que puede leer y editar este archivo mientras que el resto de usuarios sólo tiene permiso de lectura. El concepto de "items" de Reiser4 hace que sea posible dividir este archivo en un conjunto de elementos (un "item" por cada usuario) y permitir a usuarios o aplicaciones modificar sus propios datos sin acceder a los datos de otros usuarios. Este concepto favorece tanto la seguridad como la flexibilidad.

Extensiones a través de plugins Muchas de las funciones inherentes a un sistema de archivos o externas pero usadas normalmente por sistemas de archivos se han implentado en Reiser4 en forma de plugins. Si desea enriquecer

el sistema de archivos con nuevas funciones, estos plugins pueden añadirse fácilmente al sistema base sin necesidad de volver a compilar el kernel o reformatear el disco duro.

Estructura mejorada del sistema de archivos gracias a la asignación retardada
Al igual que XFS, Reiser4 soporta la asignación retardada (ver sección **??** en esta página). El uso de la asignación retardada incluso para metadatos puede resultar en una estructura global mejorada.

20.2.6. 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 (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 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 gracias a 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 asignación 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.

20.2.7. 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 hoy en día. 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" (allocation groups)
En el momento de la creación de un sistema de archivos XFS, el dispositivo de bloque (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 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.

20.3. Otros sistemas de archivos soportados

En la tabla **??** en esta página 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.

Cuadro 20.1: *Sistemas de archivos en Linux*

`cramfs`	*Compressed ROM file system*: un sistema de archivos comprimido con permiso de lectura para ROMs.
`hpfs`	*High Performance File System*: 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 tiene su origen en la universidad y fue el primero empleado en Linux. Hoy en día se utiliza como sistema de archivos para discos flexibles.
`msdos`	*fat*, el sistema de archivos empleado originariamente por DOS, es utilizado en la actualidad por varios sistemas operativos.

`ncpfs`	sistema de archivos que permite montar volúmenes Novell a través de una red.
`nfs`	*Network File System*: 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.
`smbfs`	*Server Message Block*: utilizado por productos como por ejemplo Windows para el acceso de archivos a través de una red.
`sysv`	utilizado en SCO UNIX, Xenix y Coherent (sistemas UNIX comerciales para PCs).
`ufs`	utilizado en BSD, SunOS y NeXTstep. Sólo se soporta en modo de lectura.
`umsdos`	*UNIX on MSDOS*: sistema de archivos basado en `fat` que emula las características de Unix (derechos, enlaces, nombres de archivo largos) mediante archivos especiales.
`vfat`	*Virtual FAT*: extensión del sistema de archivos `fat` (soporta nombres de archivo largos).
`ntfs`	*Windows NT file system*, sólo permiso de lectura.

20.4. 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 **??** en esta página incluye un resumen de las limitaciones actuales de los archivos y sistemas de archivos bajo Linux.

Cuadro 20.2: *Tamaño máximo de sistemas de archivos (formato en disco)*

Sist. de archivos	**Tamaño máx. archivo [Byte]**	**Tamaño máx.sist.arch.[Byte]**
Ext2 o Ext3 (1 kB tamaño bloque)	2^{34} (16 GB)	2^{41} (2 TB)
Ext2 o Ext3 (2 kB tamaño bloque)	2^{38} (256 GB)	2^{43} (8 TB)
Ext2 o Ext3 (4 kB tamaño bloque)	2^{41} (2 TB)	2^{44} (16 TB)
Ext2 o Ext3 (8 kB tamaño bloque) (sistema con páginas de 8 kB como Alpha)	2^{46} (64 TB)	2^{45} (32 TB)
ReiserFS v3	2^{46} (64 GB)	2^{45} (32 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)

Importante

Límites del kernel de Linux

La tabla ?? en esta página 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 2.6):

Tamaño de los archivos en los sistemas de 32 bits, los archivos no pueden ser mayores de 2 TB (2^{41} bytes).

Tamaño de los sistemas de archivos
los sistemas de archivos pueden tener un tamaño de hasta 2^{73} bytes, si bien todavía no existe ningún hardware que llegue hasta este límite.

Importante

20.5. Información adicional

Cada proyecto de sistema de archivos descrito arriba cuenta con su propia página web en la que puede encontrar información adicional y listas de correo, así como FAQs.

- `http://e2fsprogs.sourceforge.net/`
- `http://www.zipworld.com.au/~akpm/linux/ext3/`
- `http://www.namesys.com/`
- `http://oss.software.ibm.com/developerworks/opensource/jfs/`
- `http://oss.sgi.com/projects/xfs/`

Un completo tutorial sobre sistemas de archivos en Linux se encuentra en *IBM developerWorks*: `http://www-106.ibm.com/developerworks/library/l-fs.html` Comparación entre los distintos sistemas de archivos journaling en Linux en un artículo de Juan I. Santos Florido en *Linuxgazette*: `http://www.linuxgazette.com/issue55/florido.html`. Un detallado trabajo sobre LFS en Linux está disponible en la página de Andreas Jaeger: `http://www.suse.de/~aj/linux_lfs.html`

Autenticación con PAM

PAM (del inglés Pluggable Authentication Modules) se utiliza en Linux para gestionar la comunicación entre el usuario y la aplicación durante el proceso de autenticación. Los módulos PAM están disponibles de manera centralizada y pueden ser activados desde cualquier aplicación. El contenido de este capítulo trata acerca de cómo se configura esta autenticación modular y de cómo funciona.

Frecuentemente, los administradores de sistema y desarrolladores desean limitar el acceso a determinadas zonas del sistema o la utilización de determinadas funcionalidades de una aplicación. Sin PAM, esto significaría que todas las aplicaciones tendrían que ser adaptadas cada vez que surgiera un nuevo procedimiento de autenticación como LDAP o Samba. Este método sería muy lento y sensible a posibles fallos. Si liberamos a la aplicación del trabajo de la autenticación y asignamos esta a un módulo central, estos inconvenientes desaparecen. En caso de que tenga que emplearse un nuevo esquema de autenticación, bastará con desarrollar o adaptar un módulo PAM, el cual podrá ser empleado por todas las aplicaciones.

Para cada programa que utiliza PAM, existe un archivo de configuración propio ubicado en `/etc/pam.d/<servicio>`. En este archivo se especifica qué módulos PAM deben utilizarse para la autenticación del usuario. Los archivos de configuración globales de la mayoría de los módulos PAM (localizados en `/etc/security`) determinan el comportamiento de estos módulos (por ejemplo `pam_env.conf`, `pam_pwcheck.conf`, `pam_unix2.conf` y `time.conf`). Una aplicación que utiliza un módulo PAM ejecuta un determinado conjunto de funciones PAM. Estas tratan la información de los distintos archivos de configuración y transmiten el resultado a la aplicación que las ha iniciado.

21.1. Estructura de un archivo de configuración PAM

Una línea de un archivo de configuración PAM está compuesta, como máximo, por cuatro columnas:

```
<Tipo de módulo; <Marcador de control> <Ruta del módulo> <Opciones>
```

Los módulos PAM se procesan por lotes. Cada módulo ofrece funciones distintas. Un módulo se encarga de la comprobación de la contraseña, otro identifica desde dónde tiene lugar el acceso y otro consulta las configuraciones del sistema específicas de un usuario en concreto.

PAM reconoce cuatro tipos distintos de módulos:

`auth` Los módulos de este tipo sirven para autenticar al usuario. Esta comprobación se realiza de forma tradicional mediante la solicitud de una contraseña, aunque también puede llevarse a cabo a través de una tarjeta inteligente

equipada con un chip o mediante la comprobación de características biométricas (huella digital, escaneo de retina).

account Los módulos de este tipo comprueban si el usuario está autorizado para poder utilizar el servicio solicitado. De esta manera, se evita que un usuario pueda abrir una sesión en el sistema con una cuenta que haya expirado.

password Esta clase de módulos sirven para modificar los datos de autenticación. En la la mayoría de los casos se trata de una contraseña.

session Estos módulos están diseñados para llevar a cabo la administración y configuración de sesiones de usuario. Los módulos de este tipo se ejecutan antes y después de la autenticación a fin de registrar los intentos de inicio de sesión y proporcionar al usuario su propio entorno personalizado de trabajo (acceso al correo, directorio raíz, limitaciones del sistema etc.)

La segunda columna contiene los marcadores de control, con los que se activan los módulos deseados:

required El módulo debe ser procesado con éxito para que la autenticación pueda seguir siendo procesada. En el caso de que la ejecución de un módulo `required` genere un error, se procesará el resto de módulos de este tipo antes de que el usuario reciba un aviso de que se ha producido un problema durante su intento de autenticación.

requisite Estos módulos tienen que ser procesados con éxito del mismo modo que los módulos `required`. Si se produce un error, el usuario recibe una notificación inmediata y no se procesan más módulos. En caso de éxito, se sigue procesando el resto de módulos al igual que en el caso de los `required`. Este marcador puede configurarse como un filtro simple con el objeto de especificar el cumplimiento de determinadas condiciones, necesarias para una correcta autenticación.

sufficient Si se ejecuta con éxito un modulo de este tipo, el programa que lo ha iniciado recibe inmediatamente una notificación de éxito y no se procesa ningún otro módulo, siempre y cuando anteriormente no haya fallado la ejecución de ningún módulo `required`. El hecho de que la ejecución de un módulo `sufficient` no se complete con éxito no supone ninguna consecuencia y los módulos siguientes siguen siendo procesados por orden.

optional Su correcta ejecución o error de procesamiento no tienen ninguna consecuencia. Esta opción se utiliza, por ejemplo, en el caso de módulos que informan al usuario acerca de la recepción de un correo electrónico, pero no suponen mayores consecuencias.

include Si esta opción está presente va acompañada del archivo especificado como argumento.

La ruta del módulo no se indica explícitamente en caso de que este se encuentre en el directorio estándar `/lib/security` (o en `/lib64/security` para todas las plataformas de 64 bits soportadas por SUSE LINUX). Como cuarta columna, se puede transferir a un módulo otra opción como, por ejemplo, `debug` (modo depuración) o `nullok` (se permiten contraseñas vacías).

21.2. Configuración PAM para sshd

Una vez descritos los aspectos teóricos sobre la configuración de PAM, procederemos a describir un ejemplo práctico acerca de cómo configurar PAM para sshd:

Ejemplo 21.1: *Configuración PAM para sshd*

```
#%PAM-1.0
auth     include        common-auth
auth     required       pam_nologin.so
account  include        common-account
password include        common-password
session  include        common-session
# Enable the following line to get resmgr support for
# ssh sessions (see /usr/share/doc/packages/resmgr/README.SuSE)
#session  optional      pam_resmgr.so fake_ttyname
```

Una configuración típica de PAM para una aplicación (en este caso sshd) contiene cuatro declaraciones que corresponden a los archivos de configuración de cuatro tipos de módulos: `common-auth`, `common-account`, `common-password`, y `common-session`. Estos cuatro archivos contienen la configuración predeterminada para cada tipo de módulo. Si los incluye en lugar de activar cada módulo por separado para cada aplicación PAM, la configuración se actualizará automáticamente cada vez que el administrador cambie los valores predeterminados.

Anteriormente era necesario adaptar todos los archivos de configuración manualmente para todas las aplicaciones cada vez que PAM era modificado o se instalaba una nueva aplicación. La configuración de PAM con todos sus cambios se transmiten a través de los archivos de configuración predeterminados.

El primer archivo include (`common-auth`) activa dos módulos de tipo `auth`: `pam_env` y `pam_unix2` (ver el ejemplo **??** en esta página).

Ejemplo 21.2: *Configuración predeterminada para la sección* `auth`

```
auth    required        pam_env.so
auth    required        pam_unix2.so
```

El primer módulo, `pam_env`, lee el archivo `/etc/security/pam_env.conf` y define las variables de entorno especificadas en él. Aquí puede configurarse, por ejemplo, la variable `DISPLAY` con su valor correcto, ya que el módulo `pam_env` conoce la ubicación desde la que el usuario está intentando iniciar la sesión. El segundo módulo, `pam_unix2`, compara la contraseña y el nombre de usuario con las entradas de `/etc/passwd` y `/etc/shadow`.

Una vez que los módulos especificados en `common-auth` se han activado con éxito, un tercer módulo llamado `pam_nologin` comprueba si el archivo `/etc/nologin` existe. En caso afirmativo, sólo `root` podrá entrar al sistema. La pila completa de módulos `auth` se procesa antes de que el daemon ssh reciba una notificación respecto a si el inicio de sesión se ha realizado satisfactoriamente o no. Puesto que todos los módulos pertenecientes a la pila incorporan el marcador de control `required`, deben ser procesados con éxito para que sshd reciba un resultado positivo. En caso de que se produzca un error durante la ejecución de alguno de estos módulos, el resultado final será considerado como negativo, aunque sshd no tendrá conocimiento de ello hasta que todos los módulos de la pila hayan sido procesados.

Después de haber procesado todos los módulos de tipo `auth`, se inicia el tratamiento de otra declaración include, en este caso la mostrada en el ejemplo **??** en esta página. `common-account` contiene únicamente un módulo, `pam_unix2`. Si `pam_unix2` concluye que el usuario existe, sshd recibe un mensaje anunciando el resultado positivo y se procesa la siguiente pila de módulos (`password`) mostrada en el ejemplo **??** en esta página.

Ejemplo 21.3: *Configuración predeterminada para la sección* `account`

```
account required        pam_unix2.so
```

Ejemplo 21.4: *Configuración predeterminada para la sección* `password`

```
password required       pam_pwcheck.so  nullok
password required       pam_unix2.so    nullok use_first_pass use_authtok
#password required      pam_make.so     /var/yp
```

La configuración de PAM para sshd contiene únicamente una declaración include referente a la configuración predeterminada para los módulos `password`, la cual está incluida en `common-password`. Es necesario que estos módulos se procesen satisfactoriamente (marcador de control `required`) cada vez que la aplicación solicite el cambio de un elemento de la autenticación. La modificación de una contraseña u otro elemento de autenticación requiere una comprobación de seguridad, la cual es realizada por el módulo `pam_pwcheck`. El módulo `pam_unix2` que se utiliza posteriormente guarda las contraseñas nuevas y antiguas de `pam_pwcheck` para que el usuario no tenga que volver a autenticarse. Esto también hace que sea imposible evitar las comprobaciones realizadas por `pam_pwcheck`. Los módulos de tipo `password` deben utilizarse en los casos en los que los módulos anteriores de tipo `account` o `auth` hayan sido configurados para quejarse acerca de una contraseña caducada.

Ejemplo 21.5: *Configuración predeterminada para la sección* `session`

```
session required        pam_limits.so
session required        pam_unix2.so
```

Finalmente, los módulos del tipo `session` agrupados en el archivo `common-session` se activan para poder configurar adecuadamente las especificaciones relativas a la sesión del usuario. Aunque el módulo `pam_unix2` se inicia de nuevo, la opción `none` está seleccionada en el archivo de configuración de este módulo (`pam_unix2.conf`), por lo que su ejecución no tiene ninguna consecuencia práctica. El módulo `pam_limits` lee el archivo `/etc/security/limits.conf`, en el que pueden establecerse los límites para la utilización de algunos recursos del sistema. En caso de que el usuario cierre la sesión, se inician de nuevo los módulos `session`.

21.3. Configuración de los módulos PAM

Algunos de los módulos PAM son configurables. Los archivos de configuración correspondientes se encuentran en `/etc/security`. Este apartado trata brevemente los archivos utilizados en el ejemplo sshd. Estos son `pam_unix2.conf`, `pam_env.conf`, `pam_pwcheck.conf` y `limits.conf`.

21.3.1. pam_unix2.conf

Para llevar a cabo una autenticación mediante una contraseña tradicional, se emplea el módulo PAM `pam_unix2`. Este puede recibir sus datos desde `/etc/passwd`, `/etc/shadow`, a través de mapas NIS, desde tablas NIS+ o desde una base de datos LDAP. Las opciones de configuración pueden introducirse bien individualmente en la configuración PAM de la aplicación, o bien de manera global en `/etc/security/pam_unix2.conf`. En el ejemplo **??** en esta página se muestra un archivo de configuración muy básico para este módulo.

Ejemplo 21.6: *pam_unix2.conf*

```
auth:   nullok
account:
password:       nullok
session:        none
```

Si se selecciona la opción `nullok` en los módulos del tipo `auth` y `password`, será posible utilizar contraseñas vacías para este tipo de cuentas. El usuario está autorizado a cambiar las contraseñas. Mediante la opción `none` para el tipo `session` se determina que no se registren informes para ese tipo de módulo (configuración estándar). Si desea obtener información adicional respecto a otras opciones de configuración adicionales, consulte los comentarios en este archivo o la página del manual de pam_unix2(8).

21.3.2. pam_env.conf

Este archivo puede utilizarse para proporcionar a los usuarios un entorno estandarizado tras el inicio del módulo `pam_env`. Puede definir valores predeterminados para las variables del entorno con la siguiente sintaxis:

```
VARIABLE  [DEFAULT=[valor]]  [OVERRIDE=[valor]]
```

VARIABLE Indicador de la variable de entorno que debe ser establecido

[DEFAULT=[valor]] Valor estándar que el administrador desea definir como estándar

[OVERRIDE=[valor]] Valores que `pam_env` puede calcular y aplicar para sobreescribir el valor estándar

La variable `DISPLAY`, que se modifica cada vez que tiene lugar un login remoto, constituye un ejemplo muy común en el que el valor predeterminado ha de ser sobreescrito por `pam_env`. Ver el ejemplo **??** en esta página.

Ejemplo 21.7: *pam_env.conf*

```
REMOTEHOST     DEFAULT=localhost OVERRIDE=@{PAM_RHOST}
DISPLAY        DEFAULT=${REMOTEHOST}:0.0 OVERRIDE=${DISPLAY}
```

La primera línea determina el valor de las variables `REMOTEHOST` en `localhost`, de manera que `pam_env` no pueda calcular y devolver otro valor. La variable `DISPLAY` utiliza el valor de `REMOTEHOST`. Puede obtener más información en los comentarios del archivo `/etc/security/pam_env.conf`.

21.3.3. pam_pwcheck.conf

El módulo `pam_pwcheck` obtiene de este archivo las opciones para todos los módulos del tipo `password`. La configuración almacenada en este archivo es consultada antes que la de la aplicación PAM. En caso de que no se hubiera adoptado ninguna configuración individual para la aplicación, se utiliza la configuración global. El archivo del ejemplo **??** en esta página dice a `pam_pwcheck` que acepte contraseñas vacías y permita modificar las contraseñas. Puede consultar opciones adicionales en el archivo `/etc/security/pam_pwcheck.conf`.

Ejemplo 21.8: *pam_pwcheck.conf*

```
password:    nullok
```

21.3.4. limits.conf

El módulo `pam_limits` lee los límites del sistema para determinados usuarios o grupos del archivo `limits.conf`. En teoría, existe la posibilidad de establecer límites duros (sin posibilidad de sobrepasarlos) y blandos (se permite sobrepasarlos temporalmente) respecto a los recursos del sistema. Puede consultar la sintaxis y las opciones disponibles en el propio archivo.

21.4. Información adicional

En el directorio `/usr/share/doc/packages/pam` del sistema puede encontrar la siguiente documentación:

READMEs Puede consultar algunos READMEs generales en el nivel más alto de este directorio. Los READMEs acerca de los módulos PAM disponibles se encuentran en el subdirectorio `modules`.

The Linux-PAM System Administrators' Guide
Todo lo que necesita saber un administrador de sistemas acerca de PAM. Aquí se tratan desde cuestiones relativas a la sintaxis de un archivo de configuración PAM hasta aspectos de seguridad. Esta información está disponible en formato PDF, HTML o texto.

The Linux-PAM Module Writers' Manual
Incluye toda la información que un desarrollador necesita para programar módulos PAM conforme a los estándares aceptados por la industria. Esta información está disponible en formato PDF, HTML o texto.

The Linux-PAM Application Developers' Guide
Este documento contiene todo lo que un desarrollador de aplicaciones precisa conocer si desea utilizar las bibliotecas PAM. Esta información está disponible en formato PDF, HTML o texto.

Thorsten Kukuk ha desarrollado varios módulos de PAM para SUSE LINUX y ha publicado alguna información sobre los mismos en `http://www.suse.de/~kukuk/pam/`.

Parte III

Servicios

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 YaST. Se explica el significado de los archivos 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.

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. Para el intercambio de datos vía TCP/IP entre dos ordenadores con Linux, existen los servicios que se mencionan en la tabla **??** en esta página. Las redes basadas en TCP/IP y que están interconectadas a nivel mundial se denominan en su conjunto como "Internet.".

RFC son las siglas de *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. Los documentos RFC describen la estructura de los protocolos de Internet. Para profundizar sobre un determinado protocolo se recomienda consultar el documento RFC del protocolo correspondiente. Visite `http://www.ietf.org/rfc.html` para más información.

Cuadro 22.1: *Diferentes protocolos de la familia TCP/IP*

Protocolos	**Descripción**
TCP	(Transmission Control Protocol) 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 el 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.
UDP	(User Datagram Protocol) es un protocolo no asegurado y sin conexión. La transferencia de datos está orientada a paquetes creados directamente por 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	(Internet Control Message Protocol) 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	(Internet Group Management Protocol) es un protocolo que controla el comportamiento de los ordenadores utilizando IP multicast.

Como se muestra en la figura **??** en esta página, el intercambio de datos tiene lugar en distintas capas. En la capa de comunicación se lleva a cabo la transferencia de datos insegura a través de IP (Internet Protocol). Por encima de IP, el protocolo TCP (Transmission Control Protocol) garantiza la seguridad de la transferencia de datos hasta cierto punto. Por debajo de la capa IP se encuentra el protocolo que depende del hardware (por ejemplo Ethernet).

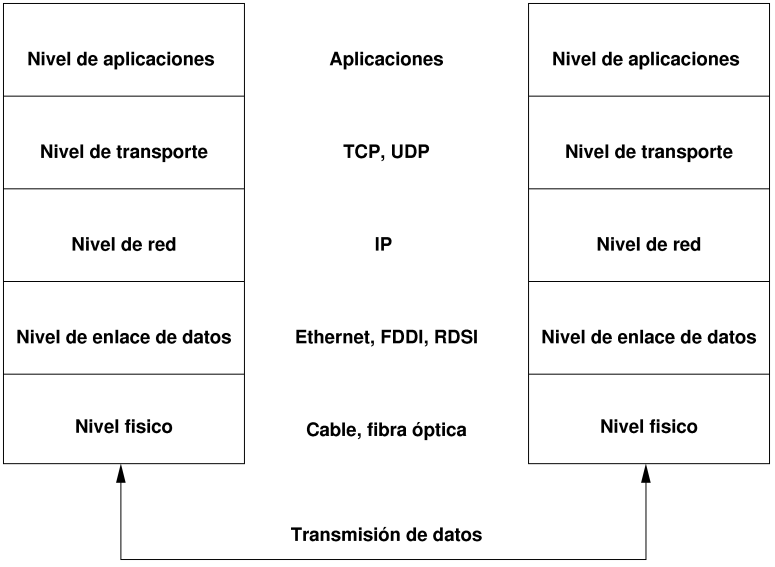

Figura 22.1: *Modelo de capas simplificado para TCP/IP*

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 mas alto. Cada capa tiene una determinada función que se explica a continuación. La red está representada por la capa de transmisión de bits y por la capa de seguridad..

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 kilobytes. En realidad los paquetes suelen tener un tamaño mucho menor, ya que el tamaño máximo de un paquete sobre una Ethernet es de 1500 bytes. Por eso el tamaño de cada paquete TCP/IP se limita a estos 1500 bytes 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.

Cada capa necesita un cierta información adicional para poder cumplir con su tarea. Esta información se encuentra en la *cabecera* (header) de cada paquete. Cada capa añade un pequeño bloque de datos (denominado "cabecera de protocolo" (protocol header) al paquete que se está formando. La figura **??** en esta página muestra el ejemplo de la composición de un paquete TCP/IP que viaja sobre un cable de una red tipo Ethernet. Una excepción de la estructura de la cabecera son los dígitos de control que no se encuentran en la cabecera sino al final. De esta forma el hardware de red lo tiene más fácil.

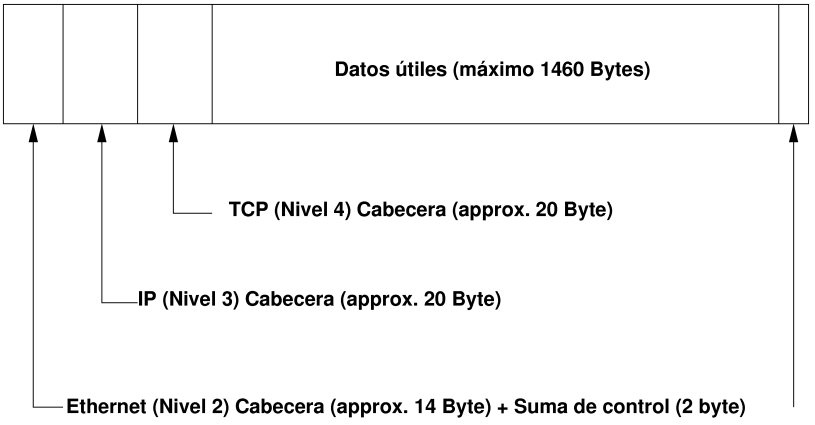

Figura 22.2: *Paquete TCP/IP sobre Ethernet*

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. Como en una cebolla, cada capa separa los encabezamientos 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 sólo se comunica con aquella que se encuentra directamente encima o 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.

22.1. Direcciones IP y routing

Las siguientes secciones se refieren a las redes IPv4. Puede obtener más información sobre su sucesor, el protocolo IPv6, en la sección **??** en esta página.

22.1.1. Direcciones IP

Cada ordenador en Internet dispone de una dirección IP única de 32 bits. Estos 32 bits o 4 bytes se representan normalmente como se muestra en la segunda fila del ejemplo **??** en esta página.

Ejemplo 22.1: *Formas de anotar una dirección IP*

```
Dirección IP (binario):   11000000 10101000 00000000 00010100
Dirección IP (decimal):   192.     168.       0.      20
```

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 posee un número único llamado *MAC* (Media Access Control). Este número es de 48 bits 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 cabecera del protocolo en la capa 2).

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" (Classless Inter Domain Routing o CIDR).

22.1.2. Máscaras de red y redes

Puesto que los ordenadores con la dirección IP 192.168.0.1 no pueden saber dónde se encuentra la máquina con la dirección IP 192.168.0.20, se crearon las máscaras de red. Simplificando se puede decir que la máscara de (sub)red define para un ordenador 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 subred) mientras que a las máquinas que estén "fuera" sólo se llega a través de un enrutador (router) o una pasarela (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: la dirección de destino se enlaza bit a bit con la máscara de red (por medio de la operación lógica Y) y la dirección del remitente se enlaza con la máscara (ver ejemplo **??** en esta página). Si existen varias interfaces de red disponibles se comprueban todas las direcciones de remitente posibles. Los resultados de los enlaces 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, cuantos más bits con valor `1` 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 una mejor compresión, la ejemplo ?? en esta página contiene algunos ejemplos.

Ejemplo 22.2: *Enlace de direcciones IP con una máscara de red*

```
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
```

La máscara de red se expresa – al igual que la dirección IP – por medio de valores decimales separados por puntos. Esta máscara es también un valor de 32 bit y por eso se anota 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 por lo general *en la misma subred* y se puede acceder a ellas directamente. Asimismo, si la Ethernet está dividida por switches o bridges, sigue siendo posible acceder directamente a estos ordenadores.

Para atravesar distancias largas, ya no se puede utilizar Ethernet sino que hace falta pasar los paquetes IP por un soporte diferente (por ejemplo FDDI o RDSI). Tales aparatos se denominan router (enrutador) o gateway (pasarela). Un ordenador con Linux también se puede encargar de ello; esta funcionalidad 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 (time to live) se haya agotado.

Cuadro 22.2: *Direcciones especiales*

Tipo de direcciones	Descripción
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 ejemplo ?? en esta página como `Resultado de la conjunción`. No se puede asignar esta dirección a ningún ordenador.

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.

No se pueden utilizar direcciones IP al azar, ya que éstas 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.

Estos tres rangos están especificados en RFC 1597 y se muestran en la tabla **??** en esta página.

Cuadro 22.3: *Rangos para direcciones IP privadas*

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`

22.2. IPv6: la próxima generación de Internet

Debido a la aparición de la WWW (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 ordena-

dores 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 la forma en que están organizadas las redes. Internet se divide en subredes. El número de direcciones disponibles en una subred es dos elevado a la potencia del número de bits menos dos. Por eso una subred se compone por ejemplo de 2, 6, 14, 30, etc. direcciones IP. Para conectar por ejemplo 128 ordenadores a Internet, se necesita una subred 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.

Para contrarrestar la previsible escasez de direcciones, en el protocolo utilizado actualmente, IPv4, se emplean mecanismos como DHCP o NAT (Network Address Translation). Ambos procedimientos atenúan relativamente la escasez de direcciones en Internet junto con la convención de zonas de direcciones de red públicas y privadas. El mayor inconveniente de estos métodos radica en su compleja configuración, que requiere además un mantenimiento muy intensivo. Para configurar un ordenador en la red IPv4 es necesario introducir numerosos datos como la dirección IP propia, la máscara de subred, dirección de la pasarela y en ocasiones incluso un servidor de nombres. Tiene que "saber" esta información que no puede deducirse de ningún sitio.

Con IPv6, la escasez de direcciones y la compleja configuración pertenecen al pasado. En las secciones siguientes le ofrecemos información adicional sobre las novedades y ventajas de IPv6 y sobre la transición del antiguo al nuevo protocolo.

22.2.1. Ventajas de IPv6

La ventaja más importante y llamativa del nuevo protocolo es la considerable ampliación del espacio direccional. Una dirección IPv6 contiene 128 bits en lugar de los tradicionales 32, con lo que el número de direcciones IP disponibles asciende a miles de billones

Las direcciones IPv6 se diferencian de sus predecesoras no sólo en la longitud, sino también en su estructura interna. Esta estructura permite codificar información especial sobre el sistema correspondiente y su red. Esta información se amplía en la sección **??** en esta página.

Entre las ventajas importantes del nuevo protocolo cabe también destacar:

Configuración automática IPv6 aplica a la red el principio "plug and play". Un sistema recién instalado puede integrarse sin problemas en la red (local). El

mecanismo automático de configuración del terminal deduce la propia dirección de la información transmitida a través del protocolo ND ("Neighbor Discovery Protocol") por los enrutadores adyacentes. Este procedimiento no requiere la intervención del administrador y tiene la ventaja adicional de que, a diferencia del distribuidor de direcciones DHCP usado en IPv4, hace innecesario el mantenimiento de un servidor central con las direcciones disponibles.

Movilidad IPv6 permite asignar varias direcciones paralelas a una interfaz de red. Esto significa para usted como usuario que puede acceder a diversas redes cómoda y fácilmente. Puede comparar este mecanismo con el "roaming" de las redes de telefonía móvil: aunque usted se encuentre en otro país, su teléfono móvil se introduce en la nueva red garantizando que siga disponible bajo el mismo número de teléfono. Usted llama por teléfono en la red externa como si se tratase de su red habitual.

Comunicación segura Mientras que en IPv4 la comunicación segura constituía una función adicional, IPv6 incluye IPSec y por tanto la comunicación segura entre dos sistemas mediante un túnel a través de Internet.

Compatibilidad con la versión anterior
No es realista creer que la migración de la totalidad de Internet de IPv4 a IPv6 se va a llevar a cabo rápidamente. Por eso es importante que ambas versiones puedan coexistir en Internet e incluso en un mismo sistema. La coexistencia de ambos protocolos en Internet está asegurada por el uso de direcciones compatibles (las direcciones IPv4 pueden convertirse fácilmente a direcciones IPv6) y la utilización de distintos "túneles" (véase la sección **??** en esta página). El uso de las direcciones IP de doble pila ("dual-stack-IP") posibilita el soporte de ambos protocolos en el mismo sistema. Cada protocolo utiliza su propia pila de red para que no se produzcan conflictos entre ambas versiones.

Multicasting: servicios a la medida Mientras que en IPv4 algunos servicios (por ej. SMB) tenían que enviar por broadcast sus paquetes a todos los miembros de la red local, IPv6 permite un procedimiento muy distinto: con multicast es posible dirigirse al mismo tiempo a un grupo de ordenadores. Es decir, no a todos (broadcast) o sólo a uno (unicast), sino a un grupo. De qué grupo se trate depende de la aplicación. No obstante, existen algunos grupos ya definidos como "todos los servidores de nombres" (all nameservers multicast group) o "todos los enrutadores" (all routers multicast group).

22.2.2. El sistema de direcciones de IPv6

Como ya se ha mencionado, el protocolo IP utilizado hasta la fecha presenta dos inconvenientes importantes. Por un lado, las direcciones IP disponibles son cada vez más escasas y por otro, la configuración de red y la administración de tablas de enrutamiento son cada vez más complicadas y requieren un gran esfuerzo de mantenimiento. IPv6 resuelve el primer problema con la ampliación del espacio de direcciones a 128 bits. En cuanto al segundo problema, la solución se encuentra en la estructura jerárquica de direcciones, los sofisticados mecanismos de asignación de direcciones en la red y la posibilidad del "multi-homing", es decir, la existencia de varias direcciones para cada interfaz con acceso a distintas redes.

En relación a IPv6 se distingue entre tres tipos de direcciones:

unicast Las direcciones de este tipo pertenecen a una única interfaz de red y los paquetes con una dirección unicast se entregan a un solo destinatario. Las direcciones de esta clase se utilizan para dirigirse a ordenadores individuales en una red local o en Internet.

multicast Las direcciones de este tipo hacen referencia a un grupo de interfaces. Los paquetes con una dirección multicast se entregan a todos los destinatarios pertenecientes a ese grupo. Este tipo de direcciones es utilizado principalmente por ciertos servicios de red para dirigirse a grupos determinados.

anycast Las direcciones de este tipo hacen referencia a un grupo de interfaces. Los paquetes con una dirección anycast se entregan a los miembros del grupo más cercano al remitente según lo determine el protocolo de enrutamiento utilizado. Las direcciones de este tipo son utilizadas por terminales para encontrar servidores que ofrezcan un servicio determinado en su sector de red. Todos los servidores reciben la misma dirección anycast. Cuando un terminal solicita un servicio, el servidor que responde es aquel que se encuentre más cercano al ordenador según el protocolo de enrutamiento empleado. Si este servidor no está disponible, se utiliza automáticamente el segundo más cercano y así sucesivamente.

Las direcciones IPv6 se representan de forma hexadecimal y están formadas por ocho bloques de 16 bits cada uno separados por dos puntos (`:`). Está permitido suprimir bytes de cero al principio, pero no en medio ni al final de un grupo. Es posible sustituir más de cuatro bytes de cero sucesivos con el comodín `::`. No se permite utilizar más de un comodín en una dirección. El proceso de suprimir los ceros se denomina en inglés "collapsing". En el ejemplo **??** en esta página se

ilustra este procedimiento a través de una misma dirección escrita de tres formas equivalentes.

Ejemplo 22.3: *Ejemplo de dirección IPv6*

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                           : 10 : 1000 : 1a4
```

Cada parte de una dirección IPv6 tiene un significado determinado. Los primeros bytes forman un prefijo que indica el tipo de la dirección. La parte central hace referencia a una red o bien no representa nada, y el final de la dirección es la parte del ordenador o host. Las máscaras de red se definen en IPv6 mediante la longitud del prefijo que se indica al final de la dirección con `/`. Según la dirección representada en el ejemplo **??** en esta página, los últimos 64 bits integran la parte del ordenador y los primeros 64 la parte de red de la dirección. En otras palabras, la cifra `64` significa que la máscara de red se rellena bit por bit comenzando por la izquierda. Por eso la máscara de red tiene 64 bits. Al igual que en IPv4, un enlace 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.

Ejemplo 22.4: *Dirección IPv6 con prefijo*

```
fe80::10:1000:1a4/64
```

IPv6 admite distintos prefijos con un significado definido (ver la tabla **??** en esta página).

Cuadro 22.4: *Diferentes prefijos IPv6*

Prefijo (hexadecimal)	Uso
`00`	Direcciones IPv4 y *compatibles con IPv4 sobre IPv6*. Son direcciones compatibles con IPv4. Un router adecuado tiene que convertir el paquete IPv6 a IPv4. Hay otras direcciones especiales (por ejemplo loopback device) que utilizan este prefijo.

Primera cifra `2` ó `3`	(Aggregatable Global Unicast Address) Igual que ahora, también en el caso de IPv6 se puede recibir la asignación de subredes a través de un proveedor. En la actualidad existen los siguientes espacios de direcciones: `2001::/16` (*production quality address space*) y `2002::/16` (*6to4 address space*).
`fe80::/10`	(link-local) Las direcciones con este prefijo no pueden ser enrutadas y por tanto sólo se puede acceder a ellas en la misma subred.
`fec0::/10`	(site-local) Estas direcciones pueden ser enrutadas pero solamente dentro de una misma organización. Estas direcciones corresponden a las direcciones "privadas" actuales (por ejemplo `10.x.x.x`).
`ff`	(multicast) Las direcciones IPv6 que comienzan por `ff` son direcciones multicast.

La estructura de las direcciones se divide en tres partes:

Public topology La primera parte, que incluye entre otras cosas uno de los prefijos mencionados en las líneas superiores, sirve para enrutar el paquete en Internet. Contiene información codificada sobre el proveedor o la institución que proporciona la conexión de red.

Site topology La segunda parte contiene información de ruta sobre la subred en la que ha de entregarse el paquete.

Interface ID La tercera parte identifica de forma unívoca la interfaz a la que va dirigida el paquete. Aquí se permite utilizar la dirección MAC como parte de la dirección, lo que simplifica enormemente la configuración del ordenador al ser una dirección única en el mundo y estar determinada por el fabricante de hardware. De hecho, los primeros 64 bits se agrupan incluso en un identificador `EUI-64` en el que los últimos 48 bits se toman de la dirección MAC y los 24 restantes incluyen información especial sobre el tipo de identificador. Esto también permite asignar un identificador `EUI-64` a dispositivos sin dirección MAC (conexiones PPP y RDSI).

Partiendo de esta estructura básica, se distinguen cinco tipos de direcciones unicast:

`::` (unspecified) Esta es la dirección de salida utilizada por un ordenador cuando su interfaz de red se inicia por primera vez y todavía no dispone de información sobre la propia dirección.

`::1` (loopback) Dirección del dispositivo loopback.

Dirección compatible con IPv4 La dirección IPv6 está compuesta por la dirección IPv4 y un prefijo de 96 bits 0 al principio de la dirección. Este tipo de direcciones compatibles se utiliza en el tunneling (ver la sección **??** en esta página). De esta forma, los ordenadores IPv4/IPv6 pueden comunicarse con otros situados en redes exclusivamente IPv4.

Direcciones IPv6 asignadas a IPv4 Este tipo de dirección indica la dirección IPv6 de un ordenador IPv4.

Direcciones locales Existen dos tipos de direcciones para el uso puramente local:

link-local Este tipo de dirección se utiliza exclusivamente en la subred local. Los enrutadores no pueden enviar los paquetes que cuenten con una dirección de salida o destino de este tipo a Internet o a otras subredes. Estas direcciones se caracterizan por un prefijo especial (`fe80::/10`) y el ID de interfaz de la tarjeta de red. La parte central de la dirección se compone de bytes 0 sin significado. Este tipo de dirección se emplea en los procesos de configuración automática para dirigirse a ordenadores en la misma subred.

site-local Este tipo de dirección puede enrutarse entre distintas subredes pero no fuera de una organización (site) hacia Internet. Estas direcciones se utilizan en intranets y equivalen a las direcciones privadas de IPv4. Además de un prefijo definido (`fec0::/10`) y del ID de interfaz, estas direcciones incluyen un campo de 16 bits en el que está codificado el ID de subred. El resto se rellena con bytes 0.

En IPv6 existe además una novedad: a una interfaz de red se le asignan por lo general varias direcciones IP, pudiendo así disponer de redes distintas. Una de ellas puede configurarse por completo automáticamente con ayuda de la dirección MAC y un prefijo conocido. De esta forma, todos los ordenadores de la red local (direcciones link-local) están disponibles inmediatamente después de iniciar IPv6 sin procesos de configuración adicionales. Gracias a las direcciones MAC integradas en las direcciones IP, estas direcciones pueden distinguirse a nivel global. Las

partes de la "Site Topology" o "Public Topology" pueden variar dependiendo de la red en la que el ordenador se encuentre en ese momento.

Si un ordenador se "mueve" entre distintas redes, necesita al menos dos direcciones. Una de ellas ("home address") contiene, además del ID de interfaz, información sobre la red local en la que funciona normalmente el ordenador y el prefijo correspondiente. La "home address" es estática y no se modifica. Todos los paquetes dirigidos a este ordenador se entregan tanto en la red local como en la externa. La entrega de paquetes en la red externa es posible gracias a importantes novedades del protocolo IPv6: *stateless autoconfiguration* y *neighbor discovery*. Además de la "home address", un ordenador móvil cuenta con una o varias direcciones adicionales pertenecientes a las redes externas en las que se mueve. Este tipo de direcciones se denomina "care-of address". La red local del ordenador móvil debe contener una instancia que "reenvíe" los paquetes dirigidos a la "home address" en caso de que el ordenador se encuentre en otra red. En entornos IPv6, esta función la realiza un "home agent" que entrega todos los paquetes dirigidos a la dirección local del ordenador móvil mediante un túnel. Aquellos paquetes cuya dirección destino sea la "care-of address" pueden ser entregados directamente a través del "home agent".

22.2.3. Coexistencia de IPv4 e IPv6

La migración de todos los ordenadores en Internet de IPv4 a IPv6 no va a producirse de la noche a la mañana, sino que ambos protocolos coexistirán durante algún tiempo. La coexistencia en un ordenador se resuelve gracias a la doble pila o "dual stack". No obstante, queda la pregunta de cómo se comunican los ordenadores IPv6 con ordenadores IPv4 y cómo se transporta IPv6 a través de las redes IPv4 aún predominantes. El método de tunneling y las direcciones compatibles (ver la sección ?? en esta página) constituyen la respuesta a estos problemas.

Las islas IPv6 individuales en medio de una red (global) IPv4 intercambian sus datos a través de túneles. Este método consiste en empaquetar los paquetes IPv6 en paquetes IPv4 para poder transportarlos a través de una red exclusivamente IPv4. Un *túnel* se define como la conexión entre dos puntos finales IPv4. Aquí debe especificarse la dirección destino IPv6 (o el prefijo correspondiente) a la que se dirigen los paquetes IPv6 encubiertos y la dirección remota IPv4 en la que han de recibirse los paquetes enviados por el túnel. En el caso más sencillo, los administradores configuran *manualmente* estos túneles entre su red y el punto destino. Este método se denomina *tunneling estático*.

Sin embargo, el método manual no siempre basta para configurar y administrar

los túneles necesarios para el trabajo diario en red. Por este motivo se han desarrollado tres métodos que permiten el *tunneling dinámico*.

6over4 Los paquetes IPv6 se empaquetan automáticamente en paquetes IPv4 y se envían a través de una red IPv4 en la que se ha activado el multicasting. De cara a IPv6 se actúa como si toda la red (Internet) fuese una única LAN (Local Area Network) de proporciones gigantescas. Así se detecta automáticamente el punto final IPv4 del túnel. Los inconvenientes de este mecanismo son una escalabilidad deficiente y el hecho de que el multicasting no está ni mucho menos disponible en toda Internet. Este método, que se describe en el RFC 2529, resulta adecuado para empresas pequeñas o redes de instituciones que dispongan de multicasting.

6to4 En este método se generan automáticamente direcciones IPv4 a partir de direcciones IPv6, permitiendo así que las islas IPv6 se comuniquen entre sí a través de una red IPv4. No obstante, también existen algunos problemas en la comunicación entre las islas IPv6 e Internet. Este método se basa en el RFC 3056.

IPv6 Tunnel Broker En este método se utilizan servidores especiales que se encargan de crear automáticamente túneles para los equipos con direcciones IPv6. Este procedimiento se describe en el RFC 3053.

Importante

La iniciativa 6Bone

En medio de la "anticuada" Internet, existe una red mundial de subredes IPv6 conectadas entre sí por medio de túneles. Dicha red se conoce como *6Bone* (`http://www.6bone.net`) y en ella se prueba IPv6. Los desarrolladores de software y proveedores que desarrollan u ofrecen servicios IPv6 pueden servirse de este entorno de pruebas para acumular experiencias con el nuevo protocolo. Puede obtener información adicional en la página web del proyecto 6Bone.

Importante

22.2.4. Configuración de IPv6

Para utilizar IPv6 normalmente no hace falta configurar nada especial en el lado del cliente. Únicamente es necesario cargar el soporte de IPv6 por ejemplo ejecutando el comando `modprobe ipv6` como usuario `root`.

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 enrutamiento en un ordenador cliente, ya que éste 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 sirve para configurar un enrutador IPv6. Este programa indica a los clientes el prefijo utilizado para las direcciones IPv6 y el/los enrutador(es) en la red. Asimismo, el programa zebra también se puede utilizar para la configuración automática de direcciones y enrutadores.

La página del manual de ifup (`man ifup`) contiene información muy útil sobre la configuración de túneles con ayuda de los archivos de `/etc/sysconfig/network`.

22.2.5. Literatura y enlaces sobre IPv6

El resumen de IPv6 presentado no pretende ser una introducción completa acerca del amplio tema IPv6. Para más información (en inglés), puede consultar la literatura impresa o en línea que se presenta a continuación:

`http://www.ngnet.it/e/cosa-ipv6.php`
Serie de artículos que describen de forma excelente los fundamentos de IPv6. Resulta muy adecuado para irse introduciendo en este tema.

`http://www.bieringer.de/linux/IPv6/`
CÓMOs de IPv6 en Linux y muchos enlaces.

`http://www.6bone.net/` Acceder a IPv6 a través de un túnel.

`http://www.ipv6.org/` Todo acerca de IPv6.

RFC 2640 El RFC introductorio sobre IPv6.

IPv6 Essentials Información general sobre IPv6. Silvia Hagen: *IPv6 Essentials*. O'Reilly & Associates, 2002. - (ISBN 0-596-00125-8).

22.3. Resolución de nombres

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* (name server). 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.

`laurent.suse.de` escrito en formato `nombre_ordenador.dominio`. Un nombre completo se denomina *nombre de dominio totalmente cualificado* (Fully Qualified Domain Name o FQDN) y se compone del nombre del ordenador y del dominio (`suse.de`). Este nombre de dominio incluye el *dominio de primer nivel* (Top Level Domain o TLD)(`de`).

Por razones históricas la asignación de los TLDs resulta algo confusa. 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. Desde el año 2000 existen TLDs adicionales para campos específicos que en ocasiones cuentan con más de 3 letras (por ejemplo `.info`, `.name`, `.museum`, etc.).

En los primeros días de Internet (antes de 1990) el archivo `/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 o un servidor de nombres no dispone de los datos de todos los ordenadores en Internet, sino que es capaz de consultar otros servidores de nombres en un nivel más alto.

En la cúspide 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 la página web `http://www.internic.net` puede encontrar más información acerca de los dominios de primer nivel gestionados por el NIC.

DNS es capaz de realizar otras tareas además 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 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 YaST 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. El capítulo ?? en esta página explica la configuración de un servidor de nombres en SUSE LINUX.

El protocolo `whois` es muy similar al de DNS y sirve para averiguar rápidamente quién se responsabiliza de un determinado dominio.

22.4. Configuración de una conexión de red mediante YaST

El ordenador debe disponer de una tarjeta red soportada. Normalmente esta es detectada durante la instalación y el controlador adecuado se activa. Se puede comprobar que la tarjeta ha sido detectada correctamente, por ejemplo, cuando la salida del comando `ip address list 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 en el archivo `/etc/sysconfig/hardware/hwcfg-*`. De no ser así, `hotplug` busca automáticamente un controlador. No se distingue entre tarjetas de red con soporte hotplug o integradas; `hotplug` se encarga de asignar los controladores en todos los casos.

22.4.1. Configuración de la tarjeta de red mediante YaST

Después de activar el módulo de YaST se mostrará un resumen de la configuración de red. En la parte superior del diálogo se muestra una lista de todas las tarjetas de red configuradas. Si su tarjeta ha sido detectada correctamente al arrancar el sistema, aparecerá mencionada aquí. Los dispositivos no reconocidos aparecen como 'Otros (no detectados)'. En la parte inferior de la vista se mencionan dispositivos ya configurados junto con el tipo y la dirección de red. Ahora puede configurar nuevas tarjetas de red o cambiar una configuración ya existente.

Configuración manual de tarjetas de red

Para configurar una tarjeta de red no detectada, realice las siguientes configuraciones básicas:

Configuración de red Especifique el tipo de dispositivo de la interfaz y el nombre de la configuración. El tipo de dispositivo se elige en un cuadro de selección mientras que el nombre de la configuración puede introducirse libremente. Los valores predeterminados suelen ser adecuados y pueden aceptarse casi siempre. Puede obtener información sobre las convenciones para los nombres de configuración en la página del manual de `getcfg`.

Módulo del kernel La opción 'Nombre de la configuración de hardware' muestra el nombre del archivo `/etc/sysconfig/hardware/hwcfg-*` donde se guarda la configuración de hardware de la tarjeta de red (por ejemplo el nombre del módulo del kernel correspondiente). YaST sugiere en la mayoría de los casos nombres adecuados para el hardware PCMCIA y USB. Para el resto del hardware, `0` se recomienda sólo si la tarjeta también se configura con `hwcfg-static-0`.

Si se trata de una tarjeta de red para un dispositivo PCMCIA o USB, active las casillas correspondientes y abandone el diálogo con 'Siguiente'. Si no es así, seleccione el modelo de su tarjeta de red mediante el botón 'Seleccionar de la lista'. YaST seleccionará automáticamente el módulo adecuado. Pulse sobre 'Siguiente' para abandonar este diálogo.

Configuración de la dirección de red

Especifique el tipo de dispositivo de la interfaz y el nombre de la configuración. El tipo de dispositivo se elige en un cuadro de selección mientras que el nombre de la configuración puede introducirse libremente. Los valores predeterminados suelen ser adecuados y pueden aceptarse casi siempre. Puede obtener información sobre las convenciones para los nombres de configuración en la página del manual de `getcfg`.

Si ha escogido 'inalámbrico' como tipo de dispositivo de la interfaz, aparecerá a continuación el diálogo 'Configuración de la tarjeta de red inalámbrica' en el que podrá determinar el modo de operación, el nombre de la red (ESSID) y la codificación. Pulse 'OK' para concluir la configuración de la tarjeta. Puede obtener una descripción detallada de las tarjetas WLAN en la sección **??** en esta página. Para el resto de tipos de interfaz, continúe con el tipo de asignación de direcciones para la tarjeta de red:

'Configuración de dirección automática (vía DHCP)'
Si dispone de un servidor DHCP en la red, éste envía automáticamente los datos de configuración para la tarjeta de red. La asignación de IP mediante

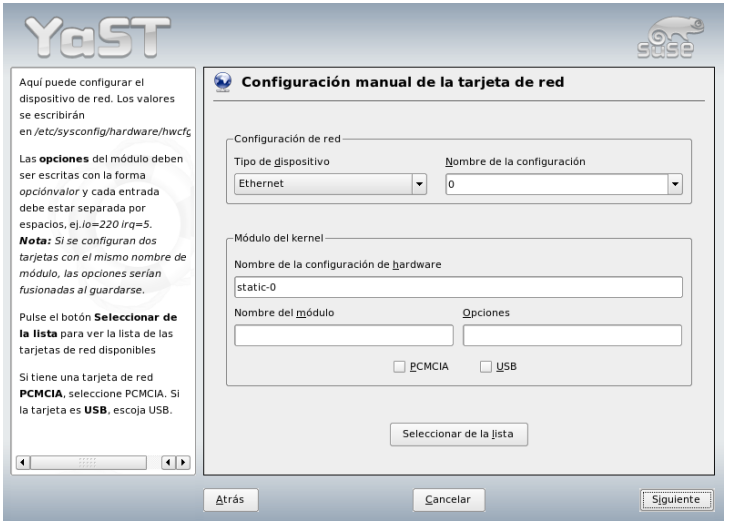

Figura 22.3: *Configuración de la tarjeta de red*

DHCP se activa también cuando el proveedor de Internet no ha notificado ninguna dirección IP estática para su sistema. Para acceder a la configuración del cliente DHCP, utilice el botón 'Opciones del cliente DHCP'. Aquí puede configurar si el servidor DHCP siempre debe reaccionar a un broadcast. También es posible asignar identificadores de tarjeta de red. Por defecto la tarjeta de red se identifica con su número MAC, pero si existen varias máquinas virtuales en un mismo PC, necesitan diferenciarse de cara al servidor.

'Configuración de direcciones estáticas'
Si dispone de una dirección IP fija, marque la casilla correspondiente. Introduzca aquí la dirección IP y la máscara de subred apropiada para la red en la que se encuentra. La configuración predeterminada de la máscara de subred resulta suficiente para una red particular típica.

Abandone este diálogo con 'Siguiente' o bien configure el nombre del ordenador, el servidor de nombres y el enrutado (ver en la página 63 y en la página 64).

El cuadro de selección 'Avanzado...' le permite definir opciones de configuración más complejas. Por ejemplo, la opción 'Controlada por el usuario' del diálogo

'Detalles…' le ofrece la posibilidad de transferir el control sobre la tarjeta de red del administrador (`root`) al usuario normal. De esta forma, los usuarios móviles pueden adaptarse de forma flexible a tipos diferentes de conexión de red, ya que ellos mismos son capaces de activar o desactivar la interfaz. Además, en este diálogo también puede definir la MTU (unidad de transmisión máxima) y el tipo de 'Activación de dispositivo'.

22.4.2. Módem

En el centro de control de YaST puede encontrar la configuración del módem en 'Dispositivos de red'. Si la detección automática no ha tenido éxito, seleccione la configuración manual e introduzca en 'Dispositivo módem' la interfaz.

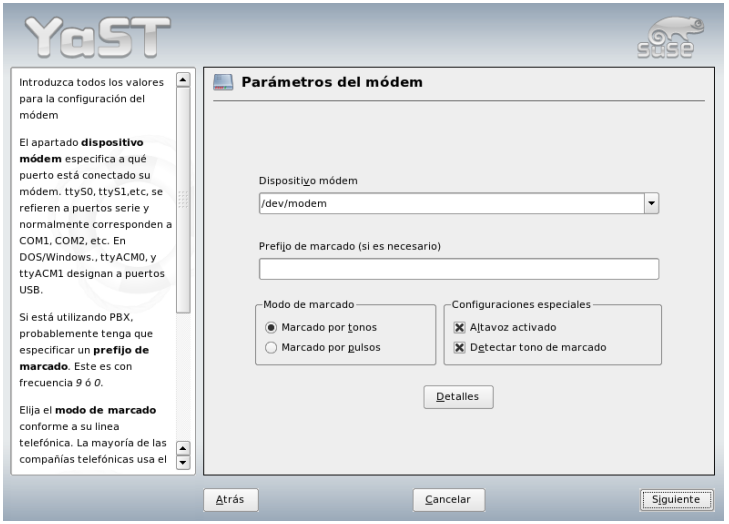

Figura 22.4: *Configuración del módem*

Si hay un sistema telefónico de marcado, para realizar llamadas al exterior es posible que deba marcar un número adicional, normalmente el cero, delante del número de teléfono . En suma, puede configurar muchas opciones, como decidir entre llamada por tonos o por pulsos o si el altavoz estará activo o si debe esperar la llamada por tonos. La última opción no se debe utilizarse si el módem está conectado a un sistema telefónico.

En la opción 'Detalles', hallará la velocidad de transferencia (en baudios) y las secuencias de inicio del módem. Cambie las opciones disponibles sólo si el módem no ha sido detectado automáticamente y si necesita ser configurado específicamente para la transmisión de datos. Este suele ser el caso de los adaptadores de terminal RDSI. Salga del diálogo con 'OK'. Si desea transferir el control sobre el módem a usuarios normales sin permisos de superusuario, active la opción 'Controlada por el usuario'. De este modo, el propio usuario puede activar o desactivar las interfaces en función de sus necesidades. A través de la opción 'Expresión regular para el prefijo de marcado' puede introducir una expresión regular con la que concuerde el 'Prefijo de marcado' definido por el usuario en KInternet . Si esta casilla permanece vacía, el usuario no tiene ninguna otra posibilidad de cambiar el 'Prefijo de marcado' sin permisos de superusuario.

En el siguiente diálogo escoja el ISP (Internet Service Provider). Si quiere seleccionar su proveedor de una lista de proveedores de su país, active el botón 'Países'. De forma alternativa, pulse el botón 'Nuevo' y aparecerá en el diálogo para determinar manualmente el parámetro ISP. Introduzca allí el nombre de marcado y del proveedor y el número de teléfono de este. Introduzca también el nombre de usuario y la contraseña que le ha suministrado el proveedor. Active la casilla 'Preguntar siempre' si quiere que se le pida la contraseña cada vez que marca.

En el último diálogo debe introducir los parámetros de conexión:

'Llamada bajo demanda' Indique al menos un servidor de nombres si quiere utilizar la llamada bajo demanda.

'Modificar DNS si conectado' Esta casilla está activada por defecto y el servidor de nombres se ajustará de forma automática cada vez que se conecta a Internet. Desactive esta opción y fije un servidor de nombres determinado si elige 'Obtención automática de DNS'.

Obtención automática de DNS En caso de que el proveedor no transmita el servidor de nombres después de la conexión, desactive esta opción e introduzca la dirección del servidor DNS manualmente.

'Modo estúpido' Esta opción está activada por defecto. Se pasarán por alto las solicitudes de servidores de marcado para facilitar el establecimiento de la conexión.

'Activar cortafuegos' Aquí puede activar el cortafuegos de SUSE y de esta forma protegerse de intrusos cuando está conectado a Internet.

'Tiempo de inactividad (segundos)' Sirve para determinar después de cuántos segundos de inactividad se debe cortar la conexión.

'Detalles IP' Con este botón aparecerá el diálogo para configurar la dirección. Si su proveedor no le ha suministrado ninguna dirección IP dinámica, desactive la casilla 'Dirección IP dinámica' e introduzca la dirección IP local de su ordenador y la dirección IP remota (su proveedor le informará de ambos datos). Deje activada la configuración de 'Ruta predeterminada' y abandone el diálogo con 'OK'.

Con 'Siguiente' volverá al diálogo en el que podrá ver lo que ha configurado. Ciérrelo finalmente con 'Finalizar'.

22.4.3. Módem cable

En ciertos países como por ejemplo Austria, EE.UU. y España, el acceso a Internet se realiza en muchas ocasiones mediante la red de televisión por cable. El usuario de este sistema recibe del operador de la red un módem cable que se conecta por una parte al cable de televisión y por otra parte – mediante 10Base-T (Twisted-Pair) – a la tarjeta de red del ordenador. Mediante el módem la máquina dispone de una línea dedicada con IP fija.

Dependiendo de las especificaciones de su proveedor, seleccione entre 'Configuración de dirección automática (vía DHCP)' o 'Configuración de la dirección estática' para la configuración de su tarjeta de red. Muchos proveedores utilizan DHCP. Los proveedores para empresas generalmente asignan una IP estática. Si este es su caso, el proveedor deberá haberle asignado una IP fija.

22.4.4. DSL

Para la configuración de una conexión por DSL, seleccione el módulo de YaST'DSL' en 'Dispositivos de red'. Aparecen varios diálogos para introducir los parámetros del acceso a Internet vía DSL. YaST le permite configurar conexiones DSL que utilizan los siguientes protocolos:

- PPP sobre Ethernet (PPPoE)
- PPP sobre ATM (PPPoATM)
- CAPI para ADSL (tarjetas Fritz)
- Protocolo de túnel para Point-to-Point (PPTP)

Tenga en cuenta que, antes de configurar el acceso DSL por PPPoE y PPTP, debe disponer de una tarjeta de red correctamente configurada. Si aún no la ha configurado, acceda a 'Configurar tarjetas de red' (ver sección **??** en esta página). La asignación de direcciones IP no se lleva a cabo con un protocolo DHCP. Por eso tampoco puede utilizar 'Configuración de dirección automática (vía DHCP)'. En su lugar asigne una dirección IP "muda" estática, `192.168.22.1` es, por ejemplo, una buena elección. En el campo 'Máscara de red' introduzca `255.255.255.0`. En el caso de un ordenador autónomo, no rellene el apartado 'Pasarela predeterminada' bajo ningún concepto.

Sugerencia

Los valores para las 'direcciones IP' del ordenador y de la 'máscara de subred' no tienen ningún valor para la conexión con ADSL y sólo son necesarios para activar la tarjeta de red.

Sugerencia

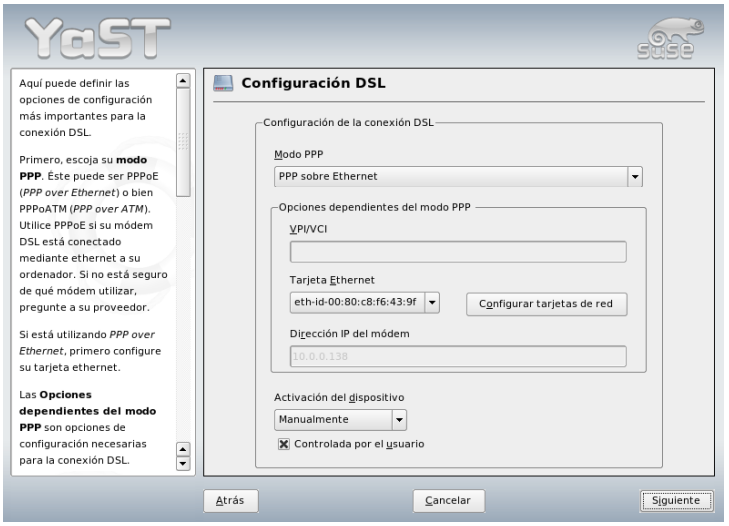

Figura 22.5: *Configuración DSL*

Al comienzo de la configuración (ver figura **??** en esta página) seleccione el modo PPP y la tarjeta Ethernet que conecta al módem (normalmente es `eth0`). La

casilla ‘Activación de dispositivo’ permite determinar si la conexión DSL se debe establecer durante el arranque del sistema o posteriormente de forma manual. La opción ‘Controlada por el usuario’ permite a los usuarios normales sin permisos de superusuario activar o desactivar interfaces por medio de KInternet. A continuación es posible seleccionar su país y el proveedor. El contenido de los diálogos posteriores depende mucho de la configuración anterior. Por eso no se explican con todo detalle. En caso de duda siempre puede consultar los textos de ayuda.

Para utilizar ‘Llamada bajo demanda’, debe configurar DNS (servidor de nombres). Hoy en día la mayoría de los proveedores soportan la asignación dinámica de DNS, lo que quiere decir que al establecer una conexión, el servidor de nombres asigna una dirección IP actual. Para ello se debe introducir en este diálogo un servidor DNS, por ejemplo `192.168.22.99`. Si no ha recibido una asignación dinámica, introduzca aquí la dirección IP del servidor de nombres de su proveedor.

Además puede configurar la cantidad de segundos de inactividad de la conexión antes de que se cancele de forma automática. Para ello active ‘Tiempo de inactividad (en segundos)’ y utilice un valor entre 60 y 300. Para evitar la cancelación de la conexión, es posible poner el tiempo de espera en 0 segundos.

22.5. Configuración manual de la red

La configuración manual de la red debería ser siempre la opción secundaria; nosotros le recomendamos utilizar siempre YaST para este propósito. No obstante, una explicación de los conceptos subyacentes a la configuración manual de la red facilitará la tarea de configuración con YaST.

Todas las tarjetas de red — ya sean integradas o dispositivos hotplug (PCMCIA, USB y parcialmente también PCI) — se detectan y configuran por medio de hotplug. Para comprender mejor este proceso, tenga presente los siguientes puntos: El sistema percibe a las tarjetas de red de dos formas. Por una parte se trata de un *dispositivo* (device) físico; por otra, actúa como *interfaz* (interface). Cuando un dispositivo es insertado o detectado, se genera un evento hotplug. Este evento hotplug hace que el dispositivo sea activado a través del script `/sbin/hwup`. Al activarse la tarjeta de red como nueva interfaz de red, el kernel produce otro evento hotplug que a su vez desencadena la configuración de la interfaz por medio de `/sbin/ifup`.

El kernel numera los nombres de interfaz en función del orden cronológico en que se han registrado. El orden de inicio es decisivo para la denominación. Si la

primera de varias tarjetas de red falla, se modifica la numeración/denominación de todas las tarjetas iniciadas con posterioridad. En el caso de tarjetas con "auténtico" soporte hotplug, lo importante es el orden en que los dispositivos han sido conectados.

Con el fin de posibilitar una configuración flexible, por una parte se ha separado la configuración de dispositivos (hardware) e interfaces y, por otra, la asignación de configuraciones a dispositivos o interfaces ya no se realiza en base a los nombres de interfaz. La configuración de los dispositivos se encuentra en `/etc/sysconfig/hardware/hwcfg-*` y la de las interfaces en `/etc/sysconfig/network/ifcfg-*`. Los nombres de las distintas configuraciones describen los dispositivos o interfaces a los que pertenecen. Puesto que la asignación de controladores a nombres de interfaces presupone que los nombres de interfaces permanezcan invariables, esta asignación ya no puede tener lugar en `/etc/modprobe.conf`. Las entradas alias en este archivo podrían tener incluso efectos secundarios negativos en el nuevo concepto.

Los nombres de configuración, es decir, todo lo que sigue a `hwcfg-` o `ifcfg-`, pueden describir a los dispositivos mediante el lugar donde están instalados, su ID específico o el nombre de interfaz. El nombre de configuració para una tarjeta PCI puede ser, por ejemplo, `bus-pci-0000:02:01.0` (ranura PCI) o bien `vpid-0x8086-0x1014-0x0549` (ID de fabricante y producto). Para la interfaz correspondiente puede utilizarse `bus-pci-0000:02:01.0` o `wlan-id-00:05:4e:42:31:7a` (dirección MAC).

Si prefiere no asignar una configuración de red determinada a una tarjeta especificada sino a cualquier tarjeta de un tipo concreto (del que sólo puede haber una tarjeta insertada en cada momento), se elige un nombre de configuración menos específico. Por ejemplo, es posible emplear `bus-pcmcia` para todas las tarjetas PCMCIA. Por otra parte, los nombres pueden restringirse un poco más anteponiéndoles un tipo de interfaz. Por ejemplo, `wlan-bus-usb` puede asignarse a todas las tarjetas WLAN con conexión USB.

Siempre se utiliza la configuración que mejor describe una interfaz o el dispositivo correspondiente a la interfaz. `/sbin/getcfg` se encarga de buscar la configuración más adecuada. La salida de `getcfg` proporciona todos los datos que pueden emplearse para describir un dispositivo. Consulte la página del manual de `getcfg` para obtener la especificación exacta de los nombres de configuración.

El método descrito permite configurar correctamente una interfaz de red de forma fiable incluso aunque los dispositivos de red no se inicien siempre en el mismo orden. No obstante, aún queda por resolver el problema de que el nombre de interfaz todavía depende del orden de activación. Existen dos formas de garantizar el acceso fiable a la interfaz de una tarjeta de red determinada:

- `/sbin/getcfg-interface` ⟨*nombre_configuración*⟩ devuelve el nombre de la interfaz de red correspondiente. Por eso también es posible introducir en algunos (por desgracia no en todos) archivos de configuración de servicios de red el nombre de la configuración en lugar del nombre de interfaz (que no es permanente). Este es el caso, por ejemplo, del cortafuegos, dhcpd, enrutamiento o diversas interfaces de red virtuales (túneles).
- Es posible asignar un nombre de interfaz permanente a todas las interfaces cuya configuración no se designa con el nombre de interfaz. Para ello se define la entrada `PERSISTENT_NAME=<pname>` en una configuración de interfaz (`ifcfg-*`). El nombre permanente ⟨*pname*⟩ no puede ser uno de los nombres que el kernel asigna automáticamente, lo que ya excluye a `eth*`, `tr*`, `wlan*`, `qeth*`, `iucv*`, etc. En su lugar puede utilizar, por ejemplo, `net*` o nombres descriptivos como `external`, `internal`, o `dmz`. Los nombres permanentes se asignan a la interfaz inmediatamente después de su registro, por lo que es necesario volver a cargar el controlador de la tarjeta de red (o bien ejecutar `hwup <descripción_dispositivo>`). En este caso no basta con ejecutar `rcnetwork restart`.

Importante

Utilizar nombres permanentes de interfaz

Tenga en cuenta que el uso de nombres permanentes de interfaz todavía no se ha probado en todas las áreas. Puede ocurrir que algunas aplicaciones no funcionen correctamente con nombres de interfaz elegidos libremente. Le agradeceríamos que nos informase de los casos en los que esto ocurra a través de `http://www.suse.de/feedback`.

Importante

`ifup` no inicia el hardware, sino que presupone la existencia de una interfaz. Para iniciar el hardware se emplea `hwup`, que es ejecutado por `hotplug` (o `coldplug`). En cuanto se inicia un dispositivo, `ifup` se inicia automáticamente para la nueva interfaz a través de `hotplug` y, si el modo de inicio es `onboot`, `hotplug` o `auto` y el servicio `network` ha sido activado, `ifup` es ejecutado. Antiguamente lo normal era que `ifup <nombre_interfaz>` desencadenase el inicio del hardware. Hoy en día el proceso es exactamente el inverso. Primero se inicia un componente de hardware y todas las acciones posteriores resultan de esta. Esto permite utilizar un juego de configuración existente para configurar de forma óptima una cantidad variable de dispositivos.

Para una mayor claridad, en la siguiente tabla se recogen los scripts más importantes que intervienen en la configuración de red. Donde sea posible se distingue entre el punto de vista del hardware y de la interfaz:

Cuadro 22.5: *Scripts para la configuración manual de la red*

Etapa de la configuración	Comando	Función
Hardware	`hw{up,down,status}`	Los scripts `hw*` son activados por el subsistema hotplug para iniciar un dispositivo, cancelar el inicio o preguntar el estado de un dispositivo. Puede obtener información adicional con `man hwup`.
Interfaz	`getcfg`	`getcfg` pregunta el nombre de interfaz correspondiente a un nombre de configuración o una descripción de hardware. Puede obtener información adicional con `man getcfg`.
Interfaz	`if{up,down,status}`	Los scripts `if*` activan o desactivan interfaces de red existentes o devuelven el estado de la interfaz en cuestión. Puede obtener información adicional con `man ifup`

Consulte el capítulo **??** en esta página y capítulo ?? en esta página para obtener más información sobre *hotplug* y los *nombres permanentes de dispositivo*.

22.5.1. Archivos de configuración

Este apartado describe de forma resumida los archivos de configuración de red disponibles así como sus funciones y formatos.

/etc/syconfig/hardware/hwcfg-*

Estos archivos contienen la configuración de hardware de las tarjetas de red y otros dispositivos. Incluyen los parámetros necesarios como por ejemplo módulo del kernel, modo de inicio y correspondencias de scripts. Puede encontrar información adicional en la página del manual de `hwup`. Los archivos de configuración `hwcfg-static-*` se aplican al iniciarse coldplug independientemente del hardware disponible en el sistema.

/etc/sysconfig/network/ifcfg-*

Estos archivos contienen la configuración de las interfaces de red e incluyen, entre otros parámetros, el modo de inicio y la dirección IP. Los parámetros posibles se describen en la página del manual de `ifup`. Asimismo, todas las variables de los archivos `dhcp`, `wireless` y `config` pueden utilizarse en los archivos `ifcfg-*` en caso de que una opción de configuración normalmente global deba utilizarse sólo para una interfaz.

/etc/sysconfig/network/config,dhcp,wireless

El archivo `config` incluye opciones de configuración generales para `ifup`, `ifdown` e `ifstatus`. Este archivo está completamente comentado. También hay comentarios en `dhcp` y `wireless`, donde se almacenan las opciones generales de configuración para DHCP y las tarjetas de red inalámbricas. También se pueden utilizar todas las variables de estos archivos en `ifcfg-*`, donde se les da preferencia.

/etc/sysconfig/network/routes,ifroute-*

Aquí se define el enrutamiento estático de los paquetes TCP/IP. En el archivo `/etc/sysconfig/network/routes` pueden introducirse todas las rutas estáticas necesarias para las diversas tareas del sistema: la ruta a un ordenador, a un ordenador a través de una pasarela o a una red. Las rutas individuales requeridas por algunas interfaces pueden introducirse en el archivo `/etc/sysconfig/network/ifroute-*`, en un archivo individual para cada interfaz. El signo `*` ha de sustituirse por el nombre de la interfaz. Las entradas podrían presentar el siguiente aspecto:

```
DESTINATION           GATEWAY NETMASK   INTERFACE [ TYPE ] [ OPTIONS ]
DESTINATION           GATEWAY PREFIXLEN INTERFACE [ TYPE ] [ OPTIONS ]
DESTINATION/PREFIXLEN GATEWAY -         INTERFACE [ TYPE ] [ OPTIONS ]
```

En caso de que no se especifiquen GATEWAY, NETMASK, PREFIXLEN o INTERFACE, debe introducirse en su lugar el signo `-`. Las entradas TYPE y OPTIONS pueden omitirse sin más.

La primera columna contiene el destino de la ruta. Dicho destino puede tratarse de la dirección IP de una red u ordenador o del nombre completo cualificado de una red u ordenador en el caso de servidores de nombres *accesibles*.

En la segunda columna aparece la pasarela predeterminada o una pasarela a través de la cual puede accederse a un ordenador o a una red. La tercera columna contiene la máscara de red de una red u ordenador detrás de una pasarela. La máscara de red para ordenadores que se encuentran detrás de una pasarela es, por ejemplo, `255.255.255.255`.

La última columna sólo tiene importancia en el caso de redes conectadas al ordenador local (loopback, Ethernet, RDSI, PPP, ...). Aquí debe aparecer el nombre del dispositivo.

/etc/resolv.conf

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. Es posible 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 pueden dar a conocer otros servidores de nombres añadiendo más líneas que comiencen con `nameserver`. Los comentarios se introducen con #. YaST escribe aquí el servidor de nombres especificado. En el ejemplo **??** en esta página, se muestra un ejemplo para `/etc/resolv.conf`.

Ejemplo 22.5: `/etc/resolv.conf`

```
# Our domain
search example.com
#
# We use sol (192.168.0.20) as nameserver
nameserver 192.168.0.20
```

Algunos servicios, como `pppd` (`wvdial`), `ipppd` (`isdn`), `dhcp` (`dhcpcd` y `dhclient`), `pcmcia` y `hotplug` pueden modificar los archivos `/etc/resolv.conf` mediante el script `modify_resolvconf`. Al modificar el archivo `/etc/`

`resolv.conf` con este script, se incluirá en el archivo un comentario con información sobre los servicios que se han modificado, el lugar donde se encuentra el archivo original y cómo es posible suprimir 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 `resolv.conf` se ha quedado modificado (por ejemplo 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 `resolv.conf` ha sido modificado, tras lo cual avisa al usuario de que se han perdido sus cambios tras la recuperación del archivo original. 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 modificaciones tienen carácter permanente mientras que las realizadas por los servicios mencionados son sólo pasajeras.

/etc/hosts

Este archivo (ver ejemplo **??** en esta página) tiene una tabla de correspondencia 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), por ejemplo `tierra`. La línea debe comenzar con la dirección IP y las demás indicaciones se separan con espacios o tabuladores. Los comentarios comienzan con #.

Ejemplo 22.6: `/etc/hosts`

```
127.0.0.1 localhost
192.168.0.20 sol.example.com sol
192.168.0.1 tierra.example.com tierra
```

/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 ejemplo **??** en esta página).

Ejemplo 22.7: /etc/networks

```
loopback     127.0.0.0
localnet     192.168.0.0
```

/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. Este sólo se utiliza para programas con enlaces a libc4 o libc5 (para programas glibc actuales, ver las opciones de configuración en `etc/nsswitch.conf`). Un parámetro debe ocupar una sola línea y los comentarios comienzan con #. Los parámetros posibles se muestran en la tabla **??** en esta página. Puede encontrar un archivo ejemplo `/etc/host.conf` en el ejemplo **??** en esta página

Cuadro 22.6: *Parámetros de /etc/host.conf*

order *hosts*, *bind*	Determina el orden de llamada a los servicios de resolución de nombres. Los parámetros posibles, separados por espacios o comas, son: *hosts*: búsqueda en el archivo `/etc/hosts` *bind*: llamada a un servidor de nombres *nis*: mediante NIS
multi *on*/*off*	Determina si un ordenador dado de alta en `/etc/hosts` puede tener varias direcciones IP.
nospoof *on* spoofalert *on*/*off*	Estos parámetros influyen sobre el *spoofing* del servidor de nombres, pero no tienen ninguna influencia adicional sobre la configuración de red.
`trim domainname`	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 `/etc/hosts` sólo contiene nombres de ordenadores locales (alias) y éstos deben ser reconocidos también cuando se añade el nombre del dominio.

Ejemplo 22.8: /etc/host.conf

```
# We have named running
order hosts bind
# Allow multiple addrs
multi on
```

/etc/nsswitch.conf

Con la version 2.0 de la librería GNU de C comenzó el uso del *Name Service Switch* (NSS) (ver la página del manual de `man 5 nsswitch.conf` o bien la información más extensa de *The GNU C Library Reference Manual*, capítulo "System Databases and Name Service Switch" – ver `libcinfo`.

El archivo `/etc/nsswitch.conf` determina en qué orden se solicitan determinadas informaciones. El ejemplo **??** en esta página muestra un archivo para `nsswitch.conf` en el que 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 capítulo ?? en esta página) después de consultar `/etc/hosts` (`files`).

Ejemplo 22.9: /etc/nsswitch.conf

```
passwd:     compat
group:      compat

hosts:      files dns
networks:   files dns

services:   db files
protocols:  db files

netgroup:   files
automount:  files nis
```

Las "bases de datos" accesibles vía NSS se recogen en la tabla **??** en esta página. Para el futuro se espera también la disponibilidad de `automount`, `bootparams`, `netmasks` y `publickey`. Las opciones de configuración para bases de datos NSS se muestran en la tabla **??** en esta página

Cuadro 22.7: *Bases de datos accesibles a través de /etc/nsswitch.conf*

`aliases`	Alias de correo, usada por `sendmail` (ver la página del manual `man 5 aliases`).
`ethers`	Direcciones de ethernet.
`group`	Usada por `getgrent` para grupos de usuarios; ver la página del manual `man 5 group`.
`hosts`	Para nombres de host y direcciones IP, utilizada por funciones como `gethostbyname` o similares.
`netgroup`	Lista de hosts y de usuarios válida en la red para administrar los derechos de acceso; ver la página del manual `man 5 netgroup`.
`networks`	Nombres y direcciones de redes, usada por `getnetent`.
`passwd`	Contraseñas de usuarios, utilizada por `getpwent`. Ver la página del manual `man 5 passwd`.
`protocols`	Protocolos de red, información utilizada por `getprotoent`. Ver la página del manual `man 5 protocols`.
`rpc`	Nombres y direcciones del tipo "Remote Procedure Call"; utilizada por `getrpcbyname` y funciones similares.
`services`	Servicios de red; datos empleados por `getservent`.
`shadow`	Las contraseñas "Shadow" de los usuarios, utilizada por `getspnam`. Ver la página del manual `man 5 shadow`.

Cuadro 22.8: *Opciones de configuración de las bases de datos NSS*

`files`	acceso directo a los archivos, por ejemplo a `/etc/aliases`.
`db`	acceso a través de una base de datos.
`nis`, `nisplus`	NIS, ver capítulo ?? en esta página.
`dns`	Parámetro adicional, solo aplicable para `hosts` y `networks`.
`compat`	Parámetro adicional para `passwd`, `shadow` y `group`.

/etc/nscd.conf

Este es el archivo para configurar nscd (Name Service Cache Daemon) - ver páginas del manual `man 8 nscd` y `man 5 nscd.conf`. La información en cuestión es la que se encuentra en `passwd` y `groups`. Es esencial para el buen rendimiento de servicios de directorio como NIS y LDAP, ya que en caso contrario cualquier acceso a nombres o grupos requeriría una conexión de red. `hosts` no se lee para no tener que reiniciar el daemon, por ejemplo, cuando se cambia la resolución de nombres de dominio (DNS) modificando `/etc/resolv.conf`.

Cuando está activada la característica "caching" para `passwd`, suelen pasar unos 15 segundos hasta que un usuario recién creado sea conocido en el sistema. Este tiempo de espera se puede reducir reiniciando nscd con el comando `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. Sólo debe contener una única línea con el nombre del ordenador.

22.5.2. Scripts de arranque

Además 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* (ver tabla **??** en esta página).

Cuadro 22.9: *Algunos scripts de arranque de las aplicaciones de red*

`/etc/init.d/network`	Este script se encarga de la configuración de las interfaces de red. Con este fin, el hardware debe haber sido iniciado a través de `/etc/init.d/coldplug` (por medio de `hotplug`). En caso de que el servicio `network` no se haya iniciado, ninguna interfaz de red será activada mediante hotplug al ser insertada.
`/etc/init.d/inetd`	Inicia xinetd. xinetd puede utilizarse para proporcionar servicios de servidor en el sistema. Así por ejemplo, puede activar vsftpd cuando se inicia una conexión FTP.
`/etc/init.d/portmap`	Inicia portmapper, el cual se necesita para utilizar servidores RPC tales como un servidor NFS.
`/etc/init.d/nfsserver`	Inicia el servidor NFS.
`/etc/init.d/sendmail`	Controla el proceso sendmail.
`/etc/init.d/ypserv`	Inicia el servidor NIS.
`/etc/init.d/ypbind`	Inicia el cliente NIS.

22.6. smpppd como asistente para la conexión 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 ipppd o pppd se encargan de controlarla. En principio, para poder estar en línea basta con iniciar estos programas correctamente.

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. Este facilita a los programas de ayuda una interfaz uniforme que funciona en dos direcciones. Por un lado programa la herramienta necesaria pppd o ipppd 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 una subred particular.

22.6.1. 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 archivo de configuración de smpppd se encuentra en `/etc/smpppd.conf`. Está configurado de tal forma que no permite el manejo remoto de manera estándar. Las opciones más interesantes de este archivo 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 debe sobrestimarse su valor como medida de seguridad. Si no se define ninguna contraseña, todos los clientes pueden acceder a smpppd.

slp-register = <yes | no> El servicio smpppd puede ser anunciado en la red a través de SLP gracias a este parámetro.

Puede encontrar más información sobre smpppd en las páginas del manual `man smpppd` y `man smpppd.conf`.

22.6.2. Configuración de kinternet, cinternet y qinternet para el uso remoto

Los programas kinternet, cinternet y qinternet pueden utilizarse para controlar un smpppd local o remoto. cinternet es el equivalente en la línea de comandos al programa gráfico kinternet. qinternet es básicamente idéntico a kinternet pero no utiliza las bibliotecas de KDE, por lo que puede utilizarse sin KDE y debe instalarse por separado. Para preparar estas herramientas para su uso con un smpppd remoto, debe editar el archivo de configuración `/etc/smpppd-c.conf` de forma manual o con kinternet. Este archivo sólo reconoce tres opciones:

sites = <list of sites> Aquí se indica a los frontales adónde dirigirse para encontrar smpppd. Los frontales probarán las opciones introducidas en el orden especificado. La opción `local` indica una conexión con el smpppd local y `gateway` con un smpppd ubicado en la pasarela. La opción `config-file` hace que la conexión se establezca como se especifica en dicho archivo en `server`. `slp` indica a los frontales que se conecten a un smpppd hallado a través de SLP.

server = <server> Aquí se puede especificar el servidor en el que se ejecuta smpppd.

password = <password> Introduzca aquí la contraseña elegida también para smpppd.

Si smpppd se está ejecutando, puede intentar acceder a él mediante el comando `cinternet --verbose --interface-list`. En caso de problemas, consulte las páginas man `man 5 smpppd-c.conf` y `man 8 cinternet`.

SLP: gestión de servicios en la red

El protocolo denominado *Service Location Protocol* (abreviado: SLP) se desarrolló para simplificar la configuración de clientes dentro de una red. Normalmente el administrador necesita un conocimiento detallado sobre los servidores en la red para realizar la configuración de un cliente de red con todos sus servicios. SLP anuncia a todos los clientes de la red la disponibilidad de un determinado servicio. Las aplicaciones que soportan SLP utilizan la información distribuida por SLP para su configuración automática.

SUSE LINUX soporta la instalación a través de SLP e incorpora muchos servicios con soporte integrado de SLP. YaST y Konqueror disponen de frontales para SLP. Se puede utilizar SLP para proporcionar a los clientes de red funciones centrales como un servidor de instalación, servidor YOU, servidor de archivos o servidor de impresión en SUSE LINUX.

23.1. Registrar servicios propios

Muchas aplicaciones de SUSE LINUX ya disponen de soporte SLP integrado gracias al uso de la librería `libslp`. Para ofrecer a través de SLP otros servicios que no incorporan soporte SLP, existen las siguiente posibilidades:

Registro estático mediante `/etc/slp.reg.d`
: Es necesario crear un archivo de registro para cada servicio nuevo. A continuación se muestra el ejemplo de un archivo que pretende registrar un servicio de escáner:

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

La línea más importante de este archivo es la *URL del servicio* (Service-URL) que comienza con `service:`. Contiene el tipo de servicio (`scanner.sane`) y la dirección en la que el servicio está disponible en el servidor. La variable ⟨*$HOSTNAME*⟩ se sustituye automáticamente por el nombre de host completo, separado por dos puntos y seguido del puerto TCP para acceder al servicio. A continuación de la URL del servicio se introducen, separados por comas, el idioma que debe utilizar el servicio para anunciarse y el tiempo de vida para el registro en el servicio (en segundos). El valor para el tiempo de vida del servicio registrado puede oscilar entre `0` y `65535`. Con `0` el registro no funciona y con `65535` no se le fija ningún límite.

El archivo de registro contiene también las variables `watch-tcp-port` y `description`. La primera opción vincula el anuncio SLP del servicio a si el servicio en cuestión está activo o no. La última variable contiene una

descripción más precisa del servicio que se muestra en un navegador adecuado.

Registro estático/`etc/slp.reg` La única diferencia con el proceso de registro ya explicado es la concentración de todos los datos dentro de un archivo central.

Registro dinámico con slptool Se puede utilizar el comando slptool para realizar el registro de un servicio SLP desde un script.

23.2. Frontales SLP en SUSE LINUX

SUSE LINUX dispone de distintas interfaces para capturar la información SLP en una red y utilizarla:

slptool slptool es un sencillo programa de línea de comandos para realizar consultas SLP en la red o para anunciar servicios propios. `slptool --help` produce una lista con todas las funciones y opciones disponibles. Se puede utilizar slptool dentro de scripts que deben procesar información SLP.

Navegador SLP de YaST YaST dispone de un navegador SLP propio al que puede accederse con 'Servicios de red' → 'Navegador SLP'. Este muestra en una estructura de árbol todos los servicios de red anunciados por SLP dentro de la red local.

Konqueror Konqueror es capaz de mostrar todos los servicios SLP de la red local cuando se introduce como URL `slp:/`. Al pulsar sobre los iconos que aparecen en la ventana principal aparece información más detallada sobre el servicio en cuestión.

Utilizando `service:/` como URL en Konqueror se muestran los iconos de los servicios en la ventana del navegador. Al pulsar sobre un determinado icono se inicia una conexión al servicio seleccionado.

23.3. Activación de SLP

Para que una ordenador pueda ofrecer servicios a través de SLP, el daemon slpd debe estar ejecutándose. Para consultar solamente la disponibilidad de un servicio no es necesario arrancarlo. Al igual que la mayoría de los servicios de sistema

de SUSE LINUX, slpd también se controla con un script de inicio. En la configuración predeterminada el daemon está inactivo. Para iniciarlo durante una sesión, ejecute como `root` el comando `rcslpd start` y `rcslpd stop` para pararlo otra vez. La opción `restart` reinicia el daemon y `status` sirve para consultar el estado del daemon. Para mantener activado slpd, ejecute una vez el comando `insserv slpd`. De esta forma, slpd pasa a formar parte de los servicios que se inician al arrancar el sistema.

23.4. Información adicional

Para obtener información más detallada sobre SLP consulte las siguientes fuentes de información:

RFC 2608, 2609, 2610 RFC 2608 contiene la definición general de SLP mientras que RFC 2609 detalla la sintaxis de las URL de servicio. RFC 2610 informa sobre DHCP a través de SLP.

http://www.openslp.com La página web del proyecto OpenSLP.

file:/usr/share/doc/packages/openslp/* Este es el directorio que contiene toda la información sobre SLP, incluyendo `README.SuSE`, que detalla las particularidades en SUSE LINUX. Se encuentran también los RFCs mencionados y dos documentos HTML introductorios. Para programar con funciones SLP, instale el paquete `openslp-devel` y utilice el *Programmers Guide* que forma parte de este paquete.

24

DNS (Domain Name System)

El servicio DNS (Domain Name System) se encarga de convertir nombres de dominio y nombres de ordenadores en direcciones IP; generalmente se habla de "resolver nombres". Antes de configurar un DNS propio consulte la información general sobre DNS en la sección **??** en esta página. Los siguientes ejemplos de configuración se refieren a BIND.

24.1. Configuración con YaST

El módulo DNS de YaST sirve para realizar la configuración de un servidor DNS dentro de la propia red local. Esta configuración basada en propuestas requiere que el administrador tome algunas decisiones básicas. Después de la configuración inicial, el servidor ya dispone de una configuración básica y en principio está listo para el uso. El modo experto ofrece opciones de configuración avanzadas como ACL, registro, claves TSIG, etc.

24.1.1. Configuración con asistente

Las propuestas del asistente o wizard se dividen en tres diálogos con la posibilidad de acceder a la configuración experta en puntos adecuados.

Instalación del servidor DNS: redireccionadores
: El diálogo de la figura **??** en esta página aparece al iniciar el módulo por primera vez. Decida si la lista de redireccionadores debe ser transmitida por el daemon PPP al conectar con DSL o RDSI ('Redireccionadores definidos por el daemon PPP') o si desea introducirla manualmente ('Definir redireccionadores manualmente').

Instalación del servidor DNS: zonas DNS
: El significado de los parámetros de este módulo se explica en la instalación para expertos (ver en esta página).

Instalación del servidor DNS: finalizar asistente
: Puesto que el cortafuegos está activado durante la instalación, al completar la misma puede abrir el puerto DNS en el cortafuegos (puerto 53). También puede determinar el comportamiento de inicio del servidor DNS o acceder desde aquí a la configuración experta (ver figura **??** en esta página).

24.1.2. Configuración experta

Al iniciar el módulo por primera vez, YaST abre una ventana con diferentes posibilidades de configuración. Una vez concluida esta configuración, el servidor DNS funciona básicamente:

Servidor DNS: inicio Bajo el título 'Arranque' se puede activar ('Encendido') o desactivar ('Apagado') el servidor DNS. Para iniciar o detener el servidor

Figura 24.1: *Instalación del servidor DNS: redireccionadores*

DNS puede emplear los botones 'Iniciar servidor DNS ahora' y 'Detener servidor DNS ahora' respectivamente. La opción 'Guardar la configuración y reiniciar el servidor DNS ahora' le permite guardar la configuración actual.

La opción 'Puerto abierto en el cortafuegos' le permite abrir el puerto DNS en el cortafuegos y con 'Configuración del cortafuegos' puede modificar las diversas opciones de configuración del cortafuegos.

Servidor DNS: redireccionadores Este diálogo es idéntico al que aparece cuando se inicia la configuración con el asistente (ver en esta página).

Servidor DNS: registro En este apartado permite determinar lo que debe protocolizar el servidor DNS y cómo debe hacerlo. En 'Tipo de registro' se especifica dónde guarda sus mensajes el servidor. Puede escribirlos en el archivo de registro del sistema en `/var/log/messages` ('Registrar al registro del sistema') o en un archivo de registro determinado explícitamente ('Registrar a archivo'). Seleccionando la última opción, se puede limitar el tamaño del archivo de registro y la cantidad de los mismos.

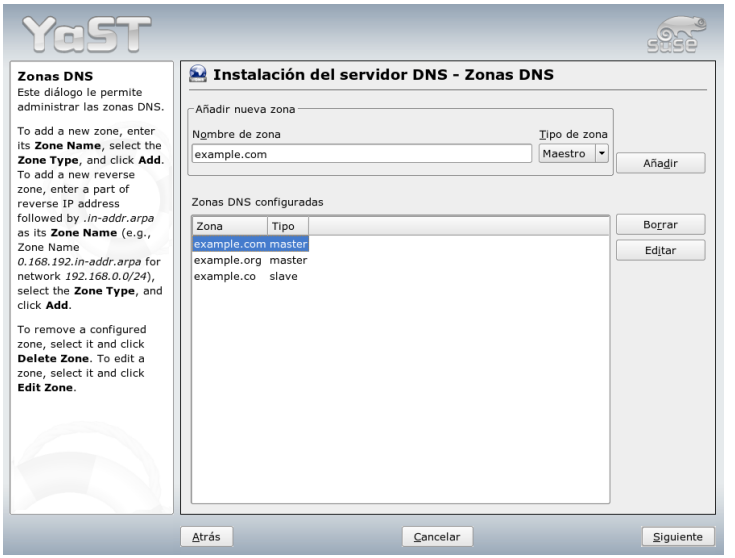

Figura 24.2: *Instalación del servidor DNS: zonas DNS*

'Registro adicional' ofrece opciones complementarias: 'Registrar solicitudes al servidor DNS' guarda en el registro *todas* las consultas, motivo por el que el archivo de registro puede llegar a ser muy voluminoso. Utilice esta opción solamente para encontrar errores. Para realizar una actualización de zona entre servidor DHCP y servidor DNS, seleccione 'Protocolar actualización de zona'. Al activar esta opción se registra el flujo de datos de maestro a esclavo a la hora de transferir los datos de zona (ver figura **??** en esta página).

Servidor DNS: zonas DNS Este diálogo, que se encarga de la administración de los archivos de zona, se divide en varias secciones (ver sección **??** en esta página). En 'Nombre de zona' puede introducir el nombre nuevo de una zona. Para crear zonas inversas, el nombre de la zona tiene que acabar en `.in-addr.arpa`. El tipo de zona (maestro o esclavo) se selecciona con 'Tipo de zona' (ver figura **??** en esta página). En 'Editar zona...' puede definir opciones adicionales para una zona existente. Para eliminar una zona seleccione la opción 'Borrar zona'.

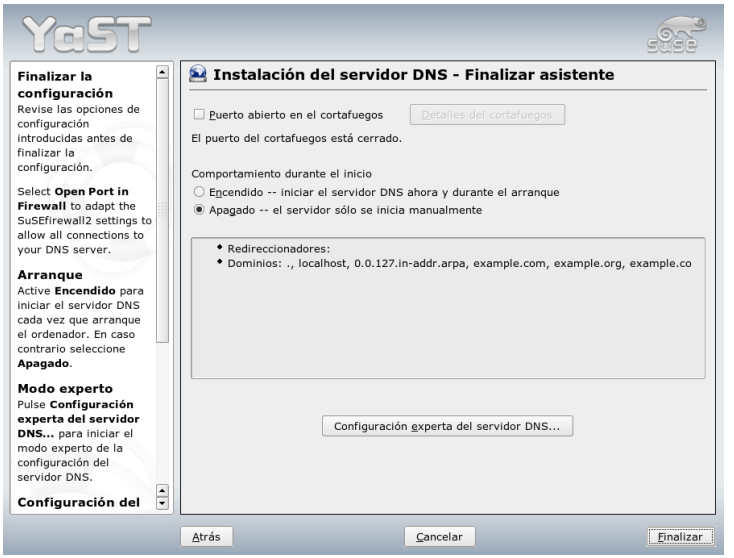

Figura 24.3: *Instalación del servidor DNS: finalizar asistente*

Servidor DNS: editor de zonas esclavas
Esta ventana de diálogo aparece cuando se selecciona 'esclava' como tipo de zona en el paso descrito en en esta página. En 'Servidor DNS maestro' indique el servidor maestro que debe ser consultado por el esclavo. Para restringir el acceso, se pueden seleccionar de la lista las ACLs creadas anteriormente (ver figura **??** en esta página).

Servidor DNS: editor de zonas maestras
Este diálogo aparece después de seleccionar 'maestra' como tipo de zona en el paso descrito en en esta página y está dividido en varias partes: fundamentos (la ventana actual), registros NS, registros MX, SOA y registros.

Servidor DNS: editor de zonas (registros NS)
Con este diálogo se puede determinar servidores de nombre alternativos para cada zona. El servidor de nombres propio tiene que estar incluido en esta lista. Para crear una nueva entrada, introduzca en 'Servidor de nombres que desea añadir' el nombre del servidor y pulse 'Añadir' (ver

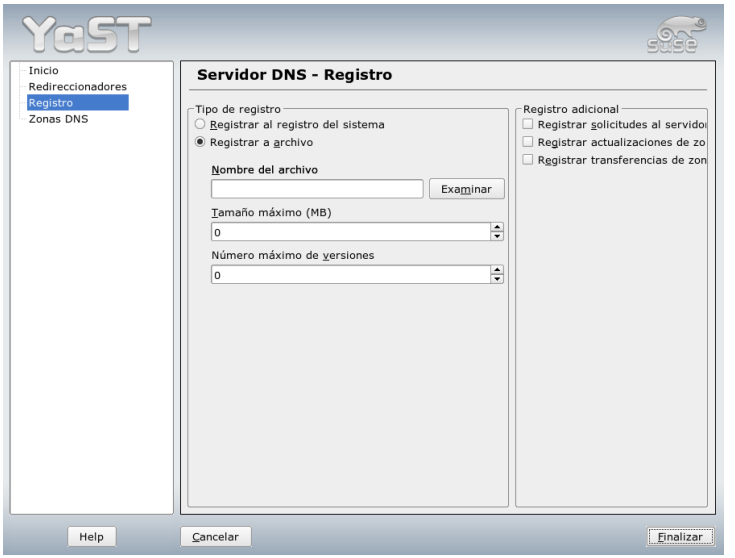

Figura 24.4: *Servidor DNS: registro*

figura **??** en esta página).

Servidor DNS: editor de zonas (registros MX)
Para añadir un servidor de correo de la zona actual a la lista existente se introduce su dirección y la prioridad. Para confirmarlo pulse 'Añadir' (ver figura **??** en esta página).

Servidor DNS: editor de zonas (SOA)
La ventana sobre Configuración del registro SOA se utiliza para crear entradas SOA (*Start of Authority*). El ejemplo ejemplo **??** en esta página muestra el significado de las opciones. En el caso de las zonas dinámicas gestionadas por LDAP no se puede crear entradas SOA.

Servidor DNS: Editor de zonas (registros)
Este diálogo administra una lista de asignaciones de nombres a direcciones IP. En el apartado 'Clave de registro' introduzca el nombre de ordenador y seleccione el tipo de registro del menú desplegable homónimo. 'Registro A' es la entrada principal, 'CNAME' es un alias y en 'MX -- reenvío de correo' el registro (nombre) se sobreescribe con el valor (value).

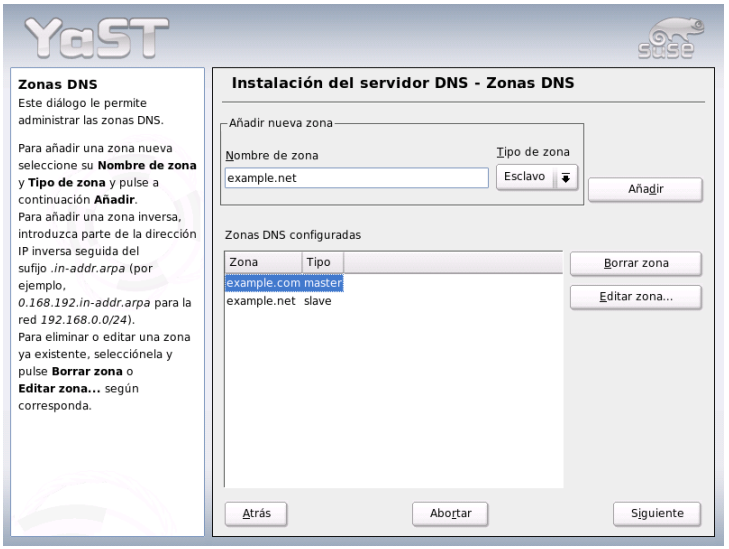

Figura 24.5: *Servidor DNS: zonas DNS*

24.2. Iniciar el servidor de nombres BIND

El servidor de nombres BIND (*Berkeley Internet Name Domain*) ya está preconfigurado en SUSE LINUX y 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 este modo BIND utiliza los servidores de nombres raíz (root name servers) para la resolución de los nombres, lo que por otra parte 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` bajo `forwarders` para conseguir una resolución de nombres eficaz y segura. Cuando funciona de esta forma, el servidor de nombres actúa en modo ”caching-only”. No se convierte en un DNS real hasta que no se configura con zonas. El directorio de documentación `/usr/share/doc/packages/bind/sample-config` incluye un ejemplo sencillo.

Figura 24.6: *Servidor DNS: editor de zonas esclavas*

Sugerencia

Adaptación automática de la configuración del servidor de nombres

Dependiendo del tipo de conexión a Internet o del entorno de red actual, la configuración del servidor de nombres puede adaptarse automáticamente a las circunstancias de cada momento. Para ello asigne el valor `yes` a la variable `MODIFY_NAMED_CONF_DYNAMICALLY` del archivo `/etc/sysconfig/network/config`.

Sugerencia

No se debería configurar ningún dominio oficial mientras este no haya sido asignado por la institución en cuestión – para ".es" ES-NIC es la organización 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, por ejemplo, el servidor web que se encuentra en el centro de datos del proveedor deja de ser ac-

Figura 24.7: *Servidor DNS: editor de zonas (registros NS)*

cesible.

El servidor de nombres puede iniciarse desde la línea de comandos como superusuario `root` 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 (llamado `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`. De no ser así, 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 comprobar si el daemon `named` está realmente en funcionamiento mediante el comando `rcnamed status` 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 este u otro en la entrada `forwarders` del apartado `options`. Las direcciones IP utilizadas en el ejemplo

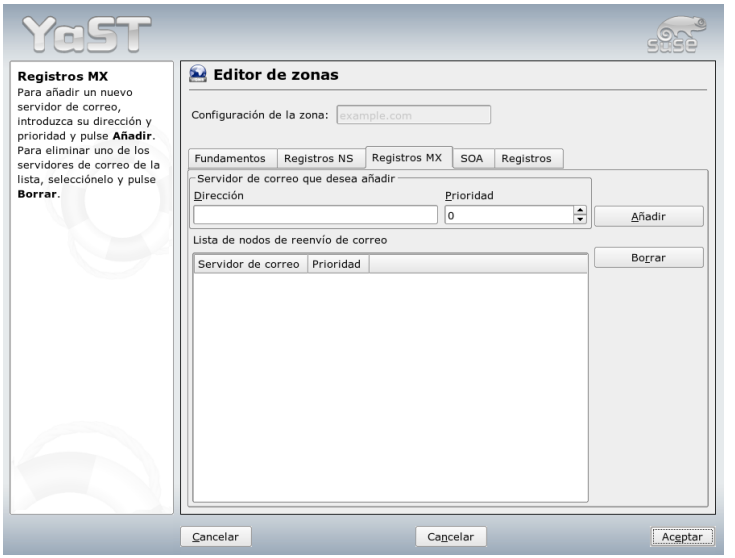

Figura 24.8: *Servidor DNS: editor de zonas (registros MX)*

?? en esta página han sido escogidas al azar y deben modificarse en función de su sistema.

Ejemplo 24.1: *Opciones de reenvío o forwarding en named.conf*

```
options {
    directory "/var/lib/named";
    forwarders { 10.11.12.13; 10.11.12.14; };
    listen-on { 127.0.0.1; 192.168.0.99; };
    allow-query { 127/8; 192.168.0/24; };
    notify no;
        };
```

Detrás de `options` se encuentran las entradas para las zonas `localhost` y `0.0.127.in-addr.arpa`. La entrada `type hint` ha de estar siempre presente. No es necesario modificar los archivos correspondientes, ya que funcionan tal y como están. Además es importante que exista un `;` al final de todas

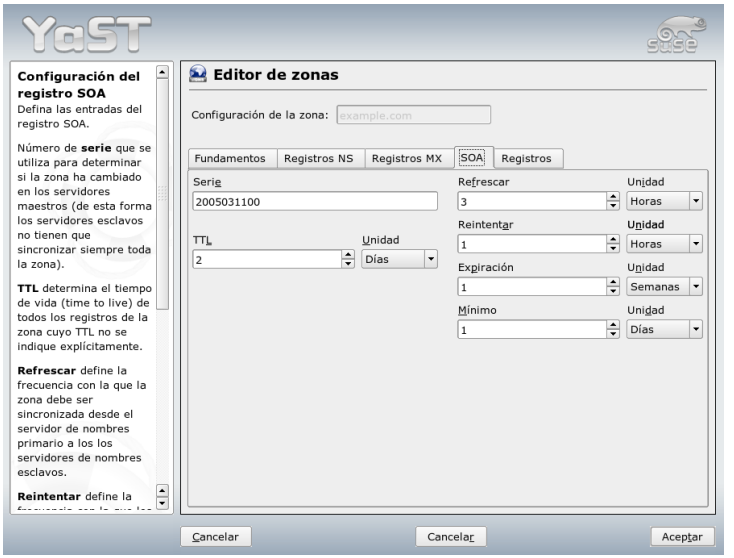

Figura 24.9: *Servidor DNS: editor de zonas (SOA)*

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`.

24.3. 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`. Esta información se ampliará en el próximo capítulo.

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` (Access Control List). Las líneas comentadas comienzan con el símbolo # o `//`. El ejemplo **??** en esta página representa un archivo `/etc/named.conf` muy sencillo.

Ejemplo 24.2: *Archivo /etc/named.conf*

```
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";
};
```

24.3.1. Información adicional sobre la configuración de BIND

directory "⟨***filename***⟩**";** especifica el directorio que contiene los archivos con los datos de zona. Este es normalmente `/var/lib/named`.

forwarders { ⟨***ip-address***⟩**; };** 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. En lugar de ⟨*ip-address*⟩ utilice una dirección IP como `10.0.0.1`.

forward first; hace que las consultas DNS se reenvíen antes de tratar de resolverlas mediante un servidor de nombres raíz. En lugar de `forward first` también es posible utilizar `forward only` para que todas las consultas sean siempre reenviadas sin acceder nunca a los servidores de nombres raíz. Esta es una opción razonable para una configuración con cortafuegos.

listen-on port 53 {127.0.0.1; ⟨*ip-address*⟩; };
indica las interfaces de red y el puerto que debe utilizar BIND para atender las peticiones DNS realizadas por los clientes. Es posible suprimir `port 53`, ya que éste es el puerto estándar. Por medio de `127.0.0.1` se autorizan las consultas del ordenador local. Si se omite esta entrada, se utilizan por defecto todas las interfaces.

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 escucha en 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 (superiores a 1024) y realiza las consultas externas 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; ⟨*net*⟩; }; determina desde qué redes está permitido hacer consultas DNS. En lugar de ⟨*net*⟩ debe introducirse una dirección como `192.168.1/24`. `/24` es una abreviatura que representa el número de bits en la máscara de red, en este caso `255.255.255.0`.

allow-transfer ! *;; determina qué ordenadores pueden solicitar transferencias de zonas. `! *` prohibe 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 escucha en 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 el reinicio del servidor de nombres no se notifica a ningún otro servidor de nombres.

24.3.2. El apartado de configuración de registro Logging

Existen muchas posibilidades de registrar eventos con BIND. Normalmente la configuración predeterminada es suficiente. El ejemplo **??** en esta página muestra la forma más sencilla de una configuración que suprime totalmente el "registro":

Ejemplo 24.3: *Registro suprimido*

```
logging {
        category default { null; };
};
```

24.3.3. Estructura de las entradas de zona

Ejemplo 24.4: *Zone Entry for my-domain.de*

```
zone "my-domain.de" in {
      type master;
      file "my-domain.zone";
      notify no;
};
```

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 ejemplo **??** en esta página. Para definir una zona esclava o *slave zone*, sólo es necesario cambiar `type` a `slave` e indicar un servidor de nombres que administre esta zona como `master` (también puede ser un "slave"); véase el ejemplo **??** en esta página.

Ejemplo 24.5: Configuración de mi-dominio.es

```
zone "otro-dominio.es" in {
      type slave;
      file "slave/otro-dominio.zone";
      masters { 10.0.0.1; };
};
```

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 servidores de nombres raíz. Es una definición de zona que no se modifica.

file `mi-dominio.zone` o file "slave/otro-dominio.zone"; Esta entrada indica el archivo que contiene los datos de zona para el dominio. En caso de un `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 { ⟨*server-ip-address*⟩; }; 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 permite 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 `! *` prohibe igualmente todo.

24.4. 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.

Sugerencia

El punto (.) en los archivos de zona

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.

Sugerencia

El primer ejemplo forma el archivo de zona `world.zone` que corresponde al dominio `world.cosmos`; véase el ejemplo **??** en esta página.

Ejemplo 24.6: *archivo /var/lib/named/world.zone*

```
1  $TTL 2D
2  world.cosmos. IN SOA      gateway  root.world.cosmos. (
3              2003072441  ; serial
4              1D          ; refresh
5              2H          ; retry
6              1W          ; expiry
7              2D )        ; minimum
8
9              IN NS       gateway
10             IN MX       10 sun
11
12 gateway     IN A        192.168.0.1
13             IN A        192.168.1.1
14 sun         IN A        192.168.0.2
15 moon        IN A        192.168.0.3
16 earth       IN A        192.168.1.2
17 mars        IN A        192.168.1.3
18 www         IN CNAME    moon
```

Línea 1: `$TTL` define el TTL estándar, que vale para todas las anotaciones de este archivo y en este caso es de 2 días (2D = 2 days).

Línea 2: Aquí comienza la parte del registro de control SOA o `SOA control record` (SOA = Start of Authority):

- En primer lugar figura el nombre del dominio a administrar `world.cosmos`, terminado con un `.` para que no se añada otra vez el nombre de la zona. Una alternativa consiste en 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 amplia a `gateway.world.cosmos` 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@world.cosmos` se escribe entonces `root.world.cosmos.`. No se debe olvidar el punto al final para que no se añada la zona.
- Al final se escribe un `(` para incorporar las siguientes líneas hasta el `)` con todo el registro SOA.

Línea 3: El número de serie en la línea `serial number` 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 rate` 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 rate` indica después de cuánto tiempo 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 `expiration time` indica el tiempo transcurrido el cual el servidor de nombres secundario debe desechar 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` especifica el servidor de nombres que se encarga de este dominio. En este caso se vuelve a convertir `gateway` en

`gateway.world.cosmos` 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 registro MX indica el servidor de correo que recibe, procesa o traspasa los mensajes para el dominio `world.cosmos`. En este ejemplo se trata del ordenador `sun.world.cosmos`. 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 valor inmediatamente superior.

Líneas 12–17: Estos son los registros de direcciones (address records) en los que se asignan una o varias direcciones IP a una máquina. Todos los nombres han sido anotados sin el punto `.` al final, de tal forma que a todos se les añade `world.cosmos`. 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 acceder a `mond` (`CNAME` es un *nombre canónico*).

Para la resolución inversa de direcciones IP (reverse lookup) se utiliza el pseudo-dominio `in-addr.arpa`. Este se añade por detrás a la parte de red de la dirección IP escrita en orden inverso. `192.168.1` se convierte así en `1.168.192.in-addr.arpa`. Consulte ejemplo **??** en esta página.

Ejemplo 24.7: *Resolución de nombres inversa*

```
1
2  $TTL 2D
3  1.168.192.in-addr.arpa. IN SOA gateway.world.cosmos. root.world.cosmos. (
4                          2003072441      ; serial
5                          1D              ; refresh
6                          2H              ; retry
7                          1W              ; expiry
8                          2D )            ; minimum
9
10                         IN NS           gateway.world.cosmos.
11
12 1                       IN PTR          gateway.world.cosmos.
13 2                       IN PTR          earth.world.cosmos.
14 3                       IN PTR          mars.world.cosmos.
```

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 `world.cosmos`.

Líneas 3–7: Véase el ejemplo anterior de `world.cosmos`.

Línea 9: Esta línea indica también el servidor de nombres responsable de la zona, pero en este caso se indica el nombre completo con el dominio y el `.` como terminación.

Líneas 11–13: Aquí se encuentran los registros de los indicadores que apuntan 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. Añadiendo 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.

24.5. Actualización dinámica de los datos de zonas

El término *actualización dinámica* se emplea para describir las operaciones relacionadas con las entradas incluidas en los archivos de zonas de un servidor maestro. Dichas operaciones pueden consistir en de añadir, modificar o eliminar datos. 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 la página del manual de `nsupdate` mediante (`man 8 nsupdate`). Por motivos de seguridad, la actualización debería realizarse a través de transacciones seguras TSIG (sección **??** en esta página).

24.6. Transacciones seguras

Las transacciones seguras pueden realizarse con ayuda de las "Transaction SIGnatures" (TSIG). Para ello se utilizan las claves de transacción (transaction keys) y las firmas de transacción (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 `man dnssec-keygen`):

dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2

Al ejecutar este comando, se crean por ejemplo los siguientes 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` se debe transmitir de forma segura (por ejemplo con `scp`) al ordenador remoto y allí introducirla en `/etc/named.conf`.

```
key host1-host2. {
 algorithm hmac-md5;
 secret ";ejIkuCyyGJwwuN3xAteKgg==;
};
```

Aviso

Permisos de acceso a `/etc/named.conf`

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`, se debe realizar 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` se deben también introducir 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`.

24.7. Seguridad DNS

DNSSEC (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 utiliza actualmente DSA. Las claves públicas (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 (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.

24.8. 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/bind/`. También se recomienda consultar los RFCs allí mencionados y las páginas del manual incluidas con BIND. `/usr/share/doc/packages/bind/README.SuSE` ofrece información actualizada de última hora acerca de BIND bajo SUSE LINUX.

Empleo de 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. Este último sirve para la distribución de sistemas de archivos en la red y se describe en el capítulo **??** en esta página.

NIS (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, por ejemplo para `/etc/hosts` o `/etc/services`, pero éstos no son objeto de discusión en estas líneas. Muchas veces se usan las letras `YP` como sinónimo de NIS; ésta es la abreviatura de *Yellow Pages*, es decir, las *páginas amarillas* en la red.

25.1. Configuración de servidores NIS

Para realizar la instalación, escoja en YaST 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 (por ejemplo 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, YaST 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 **??** en esta página), 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.

Figura 25.1: *YaST: Herramienta de configuración de un servidor NIS*

Si quiere configurar servidores esclavos NIS (*slave*) adicionales en la red, 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.

Para 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. 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`, por ejemplo de bash a sh).

Pulsando en el apartado 'Otras configuraciones globales...' accede a un diálogo (figura **??** en esta página) 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'.

Figura 25.2: *YaST: Servidor NIS: Cambiar directorios y sincronizar archivos*

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. Por eso, en los casos normales no se debe cambiar nada.

Con 'Siguiente' se llega al último diálogo en el que se puede determinar qué redes pueden realizar consultas al servidor NIS (ver figura **??** en esta página). 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.

Importante

Configuración automática del cortafuegos

Si en el sistema se está ejecutando un cortafuegos (SuSEfirewall2), YaST adapta la configuración del mismo a la del servidor NIS cuando se selecciona la opción 'Puerto abierto en el cortafuegos'. Asimismo, YaST activa el servicio `portmap`.

Importante

25.2. 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 información adicional sobre DHCP en el capítulo ?? en esta página. Si el cliente dispone de

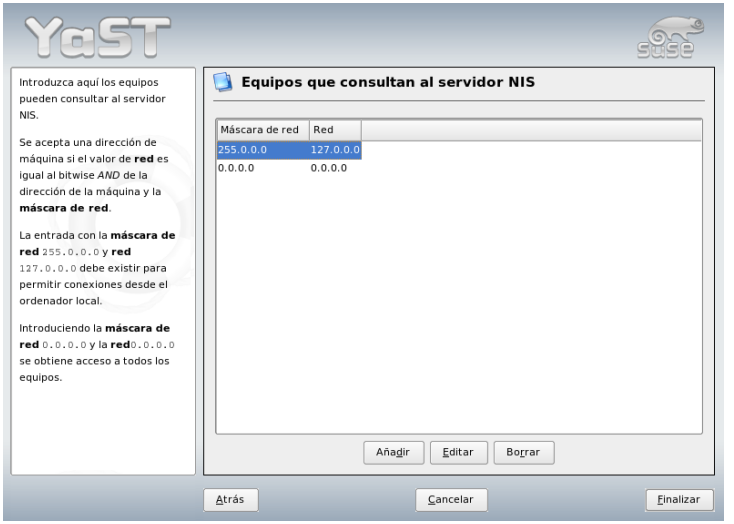

Figura 25.3: *YaST: Servidor NIS: Permiso de solicitud*

una dirección IP fija, el dominio y el servidor NIS han de introducirse manualmente (ver figura **??** en esta página) . 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 mediante el comando `man ypbind`. .

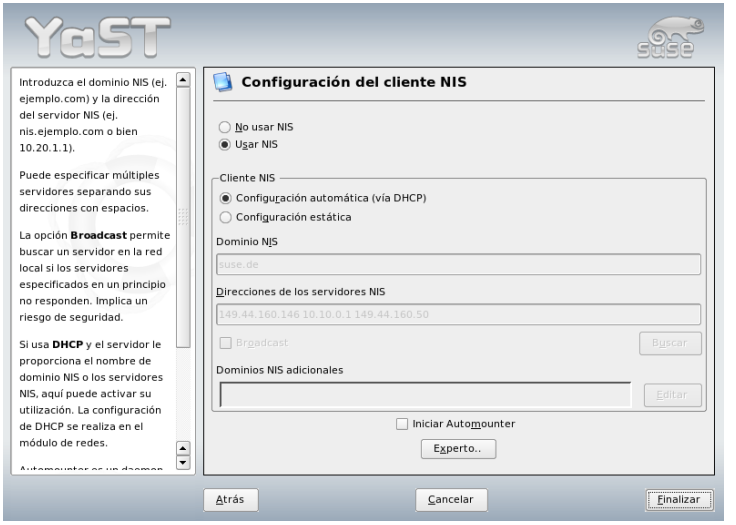

Figura 25.4: *YaST: Cliente NIS*

Compartir archivos con NFS

Como ya se ha mencionado en el capítulo ?? en esta página, 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.

Importante

Necesidad de DNS

En principio, todas las exportaciones de archivos pueden realizarse usando únicamente direcciones IP. No obstante, para evitar interrupciones por time-outs, se recomienda disponer de un sistema DNS operativo. Este es necesario al menos a efectos de registro (logging), ya que el daemon mountd realiza consultas inversas.

Importante

26.1. 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 (figura **??** en esta página).

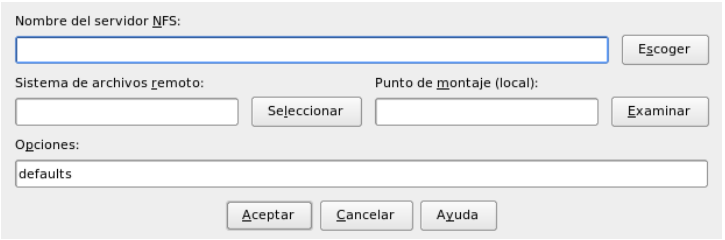

Figura 26.1: *Configuración de un cliente NFS con YaST*

26.2. 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 `rcportmap 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 host:remote-path local-path
```

Se pueden importar por ejemplo los directorios de usuario del ordenador sol con el siguiente comando:

```
mount sol:/home /home
```

26.3. Exportar sistemas de archivos con YaST

Con YaST puede convertir 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 por ejemplo 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' (figura **??** en esta página).

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 **??** en esta página). Existen cuatro opciones disponibles para los ordenadores: `single host`, `netgroups`, `wildcards` y `IP networks`. Puede encontrar una explicación más detalladas de estas opciones mediante `man exports`. Con 'Finalizar' cierra la ventana de configuración.

Figura 26.2: *Herramienta de configuración de servidores NFS*

Importante

Configuración automática del cortafuegos

Si en el sistema se está ejecutando un cortafuegos (SuSEfirewall2), YaST adapta la configuración del mismo a la del servidor NFS cuando se selecciona la opción 'Puerto abierto en el cortafuegos'. YaST activa entonces el servicio `nfs`.

Importante

26.4. Exportar manualmente sistemas de archivos

Si prescinde del apoyo de YaST, asegúrese de que los siguientes servicios estén en funcionamiento en el servidor NFS:

- RPC portmapper (portmap)

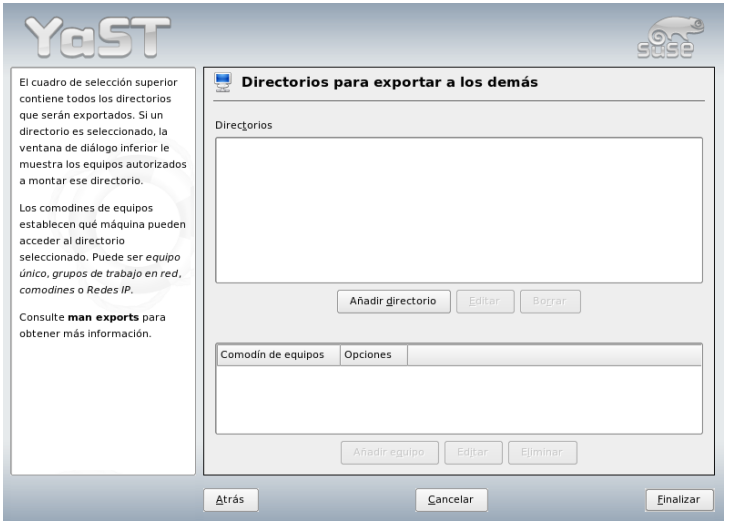

Figura 26.3: *Configuración de un servidor NFS con YaST*

- RPC mount daemon (rpc.mountd)
- RPC NFS daemon (rpc.nfsd)

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.

Cuadro 26.1: *Derechos de acceso a directorios exportados*

Opciones	Significado
`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 `root` del ordenador indicado no tenga sobre el directorio los derechos especiales típicos de `root`. Esto se logra modificando los accesos con la identidad de usuario (User-ID) `0` (`root`) al de (User-ID) `65534`. Esta identidad debe estar asignada al usuario `nobody` (esta es la opción por defecto).
`no_root_squash`	Ninguna modificación de los derechos de root.
`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 (User-ID) 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 nfsd genera una tabla para la conversión de los números de identificación de usuario. El requisito para ello es la activación del daemon ugidd.

El archivo `exports` ha de tener un aspecto similar al del ejemplo **??** en esta página. El archivo `/etc/exports` es leído por mountd y nfsd. Si modifica algo en este archivo, reinicie mountd y nfsd para que los cambios surtan efecto. Puede

hacerlo fácilmente mediante el comando `rcnfsserver restart`.

Ejemplo 26.1: */etc/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
```

DHCP

El protocolo "Dynamic Host Configuration Protocol" tiene como función proporcionar configuraciones de forma centralizada desde un servidor de la red, evitando así tener que hacerlo de forma descentralizada desde cada estación de trabajo. Una máquina configurada con DHCP no posee direcciones estáticas sino que se configura de manera totalmente 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 determinado a los clientes ”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 clientes 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) que se va a utilizar y las direcciones de los servidores de nombres. También es posible configurar de forma central algunos parámetros, como por ejemplo un servidor de tiempo, desde el cual se puede acceder a la hora actual o un servidor de impresión.

27.1. Configuración de DHCP con YaST

Al iniciar el módulo por primera vez, el administrador tiene que tomaralgunas decisiones básicas. Después de la configuración inicial el servidor está listo para arrancar y su configuración es suficiente para un escenario sencillo.

Selección de la interfaz de red Como primer paso, YaST averigua las interfaces de red del sistema. Seleccione en la lista aquella interfaz en la que el servidor DHCP debe escuchar y utilice la opción ‘Abrir cortafuegos para la interfaz seleccionada’ para determinar si el cortafuegos debe abrirse para esa interfaz (ver figura **??** en esta página).

Configuración global En las casillas de entrada puede definir la información de red que deben recibir todos los clientes que se administran desde este servidor DHCP. Esta información incluye: nombre de dominio, dirección del

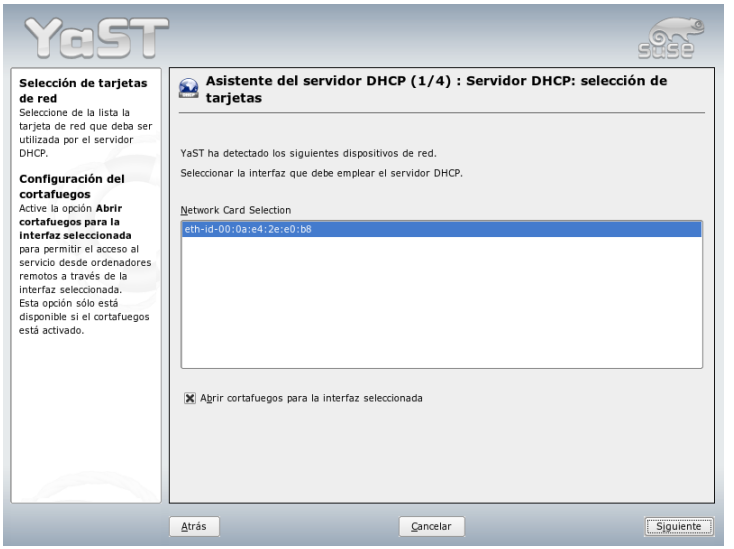

Figura 27.1: *Servidor DHCP: selección de la interfaz de red*

servidor de tiempo, dirección del servidor de nombres primario y secundario, dirección del servidor de impresión y del servidor WINS (en caso del uso simultáneo de clientes de Windows y Linux) así como la dirección de la pasarela y el tiempo de préstamo (ver figura **??** en esta página).

DCHP dinámico En este paso se configura la asignación dinámica de direcciones IP a los clientes conectados. Para ello se determina un rango de IPs al que deben pertenecer las direcciones que se van a asignar. Todas las direcciones deben estar incluidas en una máscara de red. También debe indicar el tiempo de validez durante el cual el cliente puede conservar una dirección IP sin tener que enviar una "solicitud" de prórroga. Además se puede definir el tiempo de préstamo máximo durante el cual una dirección IP concreta está reservada para un cliente determinado (ver figura **??** en esta página).

Terminar configuración y seleccionar modo de inicio
Después de haber terminado la tercera parte del asistente de configuración aparece un último diálogo acerca de las opciones de inicio del servidor

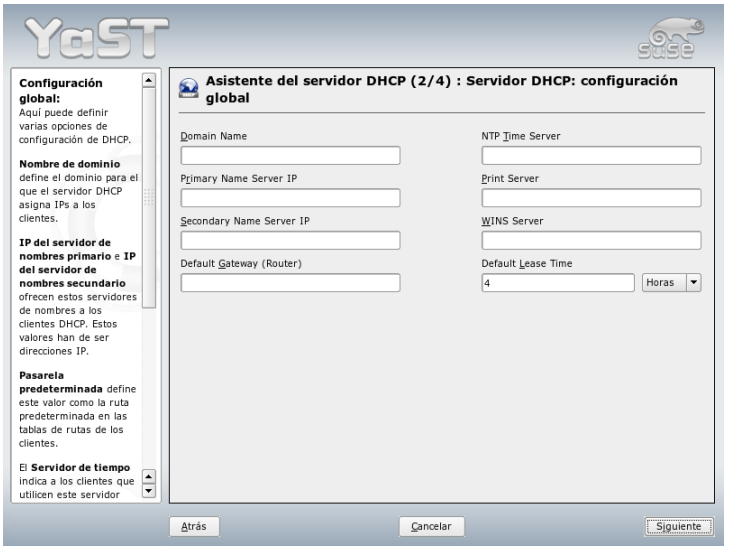

Figura 27.2: *Servidor DHCP: configuración global*

DHCP. Allí puede decidir si el servidor DHCP ha de iniciarse automáticamente cada vez que arranca el sistema ('Iniciar el servidor DHCP durante el arranque') o bien prefiere activarlo manualmente cuando sea necesario, por ejemplo con fines de pruebas ('Iniciar el servidor DHCP manualmente'). Pulse en 'Finalizar' para concluir la configuración del servidor (ver figura **??** en esta página).

27.2. Los paquetes de software DHCP

SUSE LINUX contiene tanto un servidor como clientes DHCP. El servidor DHCP dhcpd publicado por el Internet Software Consortium ofrece la función de servidor. Como clientes DHCP disponemos de dos alternativas: por un lado dhclient, también realizado por ISC, y por el otro "DHCP Client Daemon", incluido en el paquete `dhcpcd`.

dhcpcd está incluido en la instalación estándar de SUSE LINUX y su manejo es muy sencillo. Es iniciado automáticamente durante el arranque del ordenador

Figura 27.3: *Servidor DHCP: DHCP dinámico*

para buscar 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 dhclient de ISC, el cual se controla desde el archivo de configuración `/etc/dhclient.conf`

27.3. El servidor DHCP dhcpd

El *Dynamic Host Configuration Protocol Daemon* es el corazón de todo sistema DHCP. Este se encarga de "alquilar" direcciones y de vigilar su uso conforme al 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. Puede encontrar un ejemplo de un archivo `/etc/dhcpd.conf` sencillo en el ejemplo **??** en esta página:

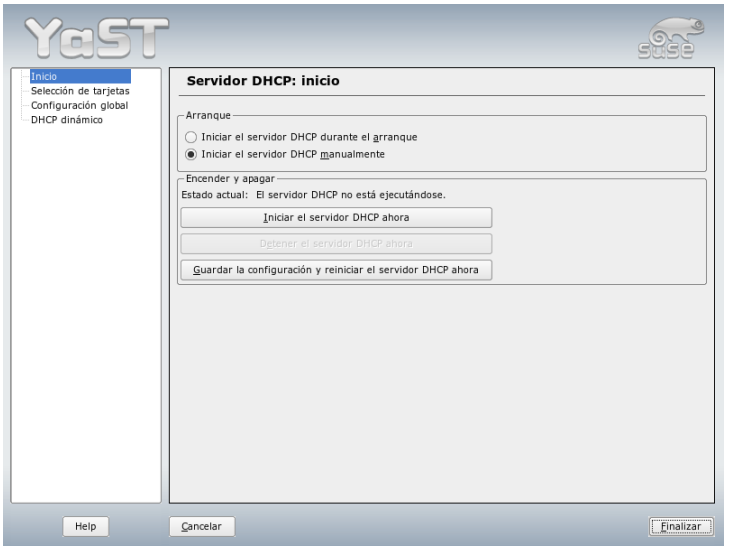

Figura 27.4: *Servidor DHCP: inicio*

Ejemplo 27.1: *El archivo de configuración /etc/dhcpd.conf*

```
default-lease-time 600;         # 10 minutes
max-lease-time 7200;            # 2  hours

option domain-name "cosmos.all";
option domain-name-servers 192.168.1.1, 192.168.1.2;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option subnet-mask 255.255.255.0;

subnet 192.168.1.0 netmask 255.255.255.0
 {
  range 192.168.1.10 192.168.1.20;
  range 192.168.1.100 192.168.1.200;
 }
```

Este sencillo archivo de configuración 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 dhcpd no arrancará.

Como se puede observar, el ejemplo anterior puede dividirse en tres bloques. En la primera parte se define de forma estándar cuántos segundos se "alquilará" una dirección IP a un cliente que lo solicite antes de que este 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 predeterminado de la red.
- En `option domain-name-servers` se pueden introducir hasta tres servidores DNS que se encargarán de resolver direcciones IP en nombres de equipo (y viceversa). Lo ideal sería que en el sistema o red hubiese ya un servidor de nombres en funcionamiento que proporcionase los nombres de equipo para las direcciones dinámicas y viceversa. Obtendrá más información sobre la creación de un servidor de nombres propio en el capítulo ?? en esta página).
- `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 ordenador de origen y 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`. Asimismo es posible comprobar 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 (Ctrl-Alt-F10) ofrecen más información.

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`.

27.3.1. Clientes con direcciones IP fijas

Como ya se ha mencionado, también existe la posibilidad de asignar a un determinado client 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 clientes que deben obtener una dirección *estática*, dhcpd se sirve de la dirección de hardware. Esta es una dirección única en el mundo para identificar las interfaces de red. Se compone de seis grupos de dos cifras hexadecimales, por ejemplo `00:00:45:12:EE:F4`. Al ampliar el archivo de configuración que se refleja en el ejemplo ?? en esta página con una entrada como se muestra en el ejemplo **??** en esta página, DHCPD siempre entrega los mismos datos al cliente correspondiente.

Ejemplo 27.2: *Ampliación del archivo de configuración*

```
host tierra {
hardware ethernet 00:00:45:12:EE:F4;
fixed-address 192.168.1.21;
}
```

El significado de estas líneas se explica prácticamente por sí mismo. Primero aparece el nombre del cliente que se va a definir (`host` ⟨*nombre_host*⟩, aquí `tierra`) y en la línea siguiente se introduce la dirección MAC. Esta es muy fácil de averiguar en Linux ejecutando el comando `ifstatus` seguido de la interfaz de red (por ejemplo `eth0`). Puede que sea necesario activar previamente la tarjeta: `ifup eth0`. Este comando produce una salida semejante a:

```
link/ether 00:00:45:12:EE:F4
```

Siguiendo el ejemplo expuesto, el cliente 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.

27.3.2. Particularidades en SUSE LINUX

Por razones de seguridad, la versión del servidor ISC DHCP incluida en SUSE LINUX incorpora el parche 'non-root/chroot' de Ari Edelkind. De este modo se consigue que dhcpd pueda ejecutarse como usuario `nobody` dentro de un entorno "chroot" (`/var/lib/dhcp`). Con este fin, el archivo de configuración `dhcpd.conf` debe copiarse en el directorio `/var/lib/dhcp/etc`, lo que es realizado automáticamente por el script de inicio durante el arranque.

Este comportamiento puede definirse en el archivo `/etc/sysconfig/dhcpd`. Para que dhcpd se ejecute sin entorno chroot, el valor de la variable `DHCPD_RUN_CHROOTED` en el archivo `/etc/sysconfig/dhcpd` ha de ser "no".

Si desea que dhcpd pueda resolver nombres de ordenador también en el entorno chroot, debe copiar a `/var/lib/dhcp/etc/` los siguientes archivos de configuración adicionales:

- `/etc/localtime`
- `/etc/host.conf`
- `/etc/hosts`
- `/etc/resolv.conf`

Estos archivos serán copiados a `/var/lib/dhcp/etc/` al iniciar el script de arranque. Los archivos han de mantenerse en un estado actualizado en caso de que sean modificados dinámicamente por un script como `/etc/ppp/ip-up`. Si el archivo de configuración contiene únicamente direcciones IP en lugar de nombres de ordenador, no habrá ningún problema.

Puede copiar varios archivos en el entorno chroot por medio del parámetro `DHCPD_CONF_INCLUDE_FILES` en el archivo `etc/sysconfig/dhcpd`. Para que el daemon dhcp siga protocolizando el registro desde el entorno chroot incluso cuando se reinicie el daemon syslog, debe añadir la opción `"-a /var/lib/dhcp/dev/log"` a la variable `SYSLOGD_PARAMS` en el archivo `/etc/sysconfig/syslog`.

27.4. Información adicional

En la página web del *Internet Software Consortium* (`http://www.isc.org/products/DHCP/`) se encuentra información adicional sobre DHCP. Además existen diversas páginas man que puede consultar. Estas son concretamente: `dhcpd`, `dhcpd.conf`, `dhcpd.leases`, y `dhcp-options`.

Sincronización horaria con xntp

El mecanismo NTP (Network Time Protocol) puede definirse como un protocolo para sincronizar la hora del sistema a través de la red. Este protocolo permite tanto que una máquina obtenga la hora de una fuente horaria fiable (un servidor) como que sea la propia máquina la que actúe como fuente horaria para otros ordenadores de la red. El objetivo consiste en mantener la hora absoluta y sincronizar la hora del sistema de todas las máquinas en una red.

La hora exacta juega un papel primordial en muchos de los procesos que tienen lugar en un sistema informático. El reloj de hardware integrado (BIOS) no siempre satisface los requisitos exigidos por aplicaciones como las bases de datos. Es posible que la corrección manual de la hora del sistema ocasione graves problemas. Así por ejemplo, el atrasar la hora podría provocar fallos en el funcionamiento de aplicaciones críticas. Aunque normalmente es necesario sincronizar la hora de todos los equipos de una red, el ajuste manual no es el método más recomendable para ello. xntp representa un planteamiento mucho más adecuado para resolver este problema. Por una parte, xntp utiliza servidores de tiempo en la red para corregir la hora local de forma permanente. Por otra, xntp permite administrar referentes locales de tiempo como por ejemplo relojes controlados por radio.

28.1. Configuración de xntp en la red

En su configuración predeterminada, xntp utiliza el reloj local del ordenador como referente horario. Sin embargo, el reloj de la BIOS sólo debería utilizarse como reloj de reserva para casos en los que no esté disponible otra fuente horaria más precisa. La forma más sencilla de utilizar un servidor de tiempo en la red consiste en definir parámetros de servidor. Por ejemplo, si desde la red puede accederse a un servidor de tiempo llamado `ntp.example.com`, podemos añadirlo al archivo `/etc/ntp.conf` introduciendo en él la línea `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`, la hora se estabiliza y se crea el archivo "drift" para corregir el reloj local del ordenador. Gracias al archivo "drift", el error sistemático del reloj de hardware puede calcularse en cuanto se enciende el ordenador. La corrección se activa inmediatamente con lo que se consigue un tiempo de máquina muy estable.

Existen dos formas de utilizar el mecanismo NTP como cliente: en la primera, el cliente solicita la hora a un servidor conocido a intervalos regulares. En caso de que haya muchos clientes, este método puede ocasionar una gran carga en el servidor. En segundo lugar, el cliente puede esperar a que le lleguen broadcasts NTP enviados por servidores de tiempo de la red. El inconveniente de este método radica en que la calidad del servidor no se conoce con seguridad y un servidor que envíe información errónea puede provocar problemas importantes.

Si la hora se obtiene por broadcast, no es necesario que cuente con un servidor de nombres. En este caso introduzca la línea `broadcastclient` en el archivo de

configuración /etc/ntp.conf. Para utilizar exclusivamente uno o varios servidores de tiempo conocidos, introduzca sus nombres en la línea que comienza con servers.

28.2. Instalar un reloj de referencia local

El paquete xntp contiene 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. La letra t representa el tipo de reloj y determina el controlador utilizado, mientras que la u significa unidad y especifica la interfaz empleada.

Cada controlador dispone normalmente de parámetros especiales que definen la configuración con más detalle. El archivo /usr/share/doc/packages/xntp-doc/html/driverNN.htm (donde NN equivale al número de controlador) proporciona información sobre un tipo de reloj determinado. Por jemplo, para un reloj de "tipo 8" (reloj controlado por radio a través de puerto serie) 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. De acuerdo con esto, 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 el sistema en el directorio /usr/share/doc/packages/xntp-doc/html. El archivo /usr/share/doc/packages/xntp-doc/html/refclock.htm contiene enlaces a páginas de controladores donde se describen los parámetros disponibles.

28.3. Configuración de un cliente NTP con YaST

Además de esta configuración manual, SUSE LINUX también soporta la configuración de un cliente NTP por medio de YaST. Puede optar entre una configuración rápida y sencilla y una 'Configuración compleja'. A continuación se describen ambos tipos de configuración.

28.3.1. Configuración rápida de un cliente NTP

La configuración sencilla del cliente NTP comprende únicamente dos diálogos. En el primer diálogo puede definir el modo de inicio de xntpd y el servidor al que se van a realizar consultas. Para activarlo automáticamente durante el arranque escoja la opción 'Al arrancar el sistema'. Pulse 'Seleccionar' para detectar un servidor de tiempo adecuado para su red. A continuación se abre un segundo diálogo más detallado para seleccionar el servidor.

Figura 28.1: *YaST: configuración de un cliente NTP*

En el diálogo detallado para seleccionar el servidor debe definir en primer lugar si desea sincronizar la hora con un servidor de la red propia o con un servidor de tiempo de Internet responsable de su zona horaria (botón 'Servidor NTP público'). En el primer caso, pulse 'Consulta' para iniciar una búsqueda SLP de servidores de tiempo disponibles en la red local. Seleccione un servidor de la lista de resultados y salga del diálogo con 'OK'. En el caso del servidor NTP público, seleccione primero su país (zona horaria) en el diálogo 'Servidor NTP público' y escoja un servidor adecuado de la lista que aparece a continuación. Para completar la configuración pulse los botones 'OK' y 'Finalizar' después de haber comprobado la disponibilidad del servidor con 'Probar'.

28.3.2. Configuración compleja de un cliente NTP

Para acceder a la configuración compleja de un cliente NTP seleccione en primer lugar el modo de inicio como se ha descrito en la configuración rápida y escoja la opción 'Configuración compleja' del diálogo de inicio del 'Cliente NTP' (ver figura **??** en esta página).

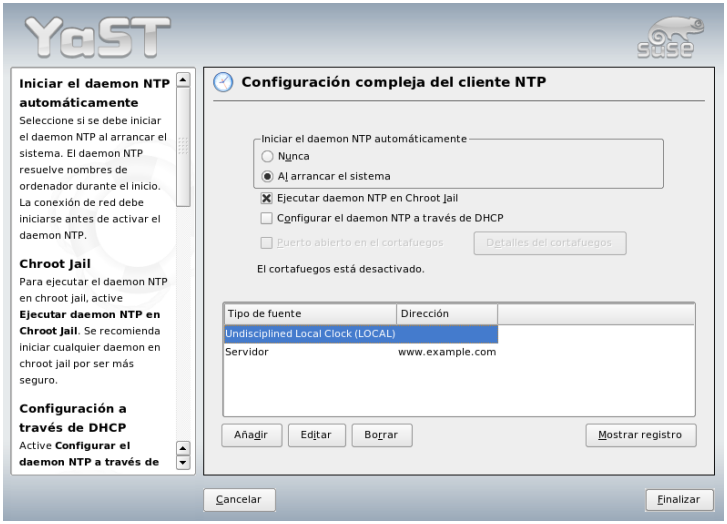

Figura 28.2: *YaST: configuración compleja de un cliente NTP*

En el diálogo 'Configuración compleja del cliente NTP' puede especificar si xntpd

debe iniciarse en un entorno chroot-jail. Esta opción incrementa la seguridad en caso de un ataque a través de xntpd, ya que el atacante no puede poner en peligro todo el sistema. Además dispone de la opción 'Configurar el daemon NTP a través de DHCP' para configurar el cliente NTP de tal forma que se le informe mediante DHCP de la lista de servidores NTP disponibles en la red.

En la parte inferior del diálogo se muestran las fuentes de información que consultará el cliente. Esta lista puede editarse con los botones 'Añadir', 'Editar' y 'Borrar'. La opción 'Avanzado' le permite examinar los archivos de registro del cliente o ajustar el cortafuegos a la configuración del cliente NTP.

Pulse el botón 'Añadir' para añadir una nueva fuente para la sincronización horaria. A continuación se abre un diálogo en el que debe seleccionar el tipo de fuente. Los tipos de fuente disponibles son los siguientes:

Servidor En un diálogo posterior podrá seleccionar el servidor NTP (como se ha descrito en la sección **??** en esta página). La opción 'Usar para la sincronización inicial' puede activarse para que la sincronización horaria entre servidor y cliente tenga lugar durante el arranque. Otra casilla de texto le permite introducir opciones adicionales para xntpd. Puede obtener más información al respecto en `/usr/share/doc/packages/xntp-doc`.

Conector Un conector (peer) es una máquina con la que se establece una relación simétrica, es decir, que actúa como servidor de tiempo y como cliente. Para utilizar un conector para la sincronización en lugar de un servidor, introduzca la dirección del sistema en cuestión. El resto del diálogo es idéntico al de 'Servidor'.

Reloj de radio Si dispone de un reloj de radio en el sistema y desea utilizarlo para la sincronización horaria, introduzca en este diálogo el tipo de reloj, número y nombre de dispositivo y el resto de opciones. La opción 'Calibración del controlador' le permite configurar de forma detallada el controlador correspondiente. Puede obtener información adicional sobre el funcionamiento de un reloj de radio en `/usr/share/doc/packages/xntp-doc/html/refclock.htm`.

Broadcasting Las consultas y la información relativa a la hora pueden enviarse a la red a través de broadcasts. Introduzca en este diálogo las direcciones que han de recibir dichos broadcasts. Active esta opción sólo si dispone de una fuente horaria fiable como por ejemplo un reloj controlado por radio.

Aceptando paquetes broadcast Si desea que el cliente reciba la información enviada por broadcast, introduzca aquí la dirección de la que deben aceptarse los paquetes correspondientes.

El servicio de directorio LDAP

LDAP (Lightweight Directory Access Protocol) es un conjunto de protocolos diseñados con el fin de acceder y mantener directorios de información. LDAP puede ser empleado para varios propósitos, tales como la gestión de usuarios y grupos, de la configuración del sistema o de las direcciones. Este capítulo le ofrece una descripción básica acerca de cómo funciona LDAP y cómo puede administrarse mediante YaST.

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 servicios de directorio son la respuesta a este problema. De manera semejante a las páginas amarillas (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 (Lightweight Directory Access Protocol) garantiza que el mayor número posible de aplicaciones de clientes tenga acceso a esta información.

En este contexto, 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, NDS de Novell, ADS de Microsoft, Street Talk de Banyan y el estándar OSI X.500. Originalmente, LDAP fue planeado como una variante más simple de DAP (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 (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`

29.1. LDAP versus NIS

Tradicionalmente, los administradores de sistemas Unix utilizan el servicio NIS para la resolución de nombres y distribución de datos en la red. Los da-

tos 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.

29.2. 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` (country), `ou` (OrganizationalUnit), y `dc` (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` (country), `dc` (domainComponent) o `o` (organization).

El siguiente ejemplo ilustra mejor las relaciones jerárquicas dentro de un árbol de directorios LDAP (ver figura **??** en esta página).

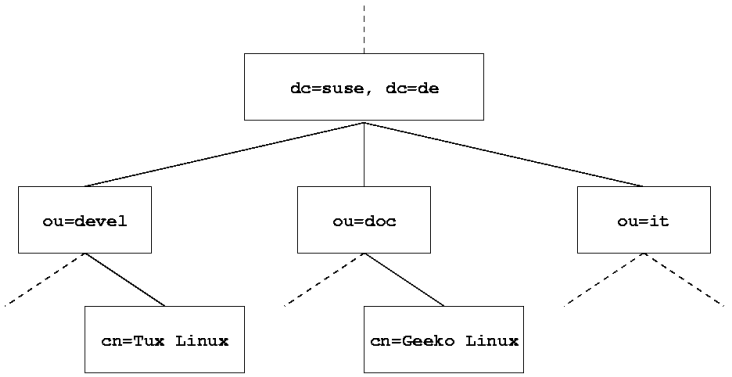

Figura 29.1: *Estructura de un directorio LDAP*

La figura representa un DIT ficticio con entradas (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 SUSE `Geeko Linux` es `cn=Geeko Linux,ou=doc,dc=suse,dc=de`. Este nombre

se forma al añadir el RDN `cn=Geeko Linux` al DN de la entrada precedente `ou=doc,dc=suse,dc=de`.

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 **??** en esta página 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.

Cuadro 29.1: *Clases de objetos y atributos de uso extendido*

Clase de objeto	Significado	Entrada de ejemplo	Atributo obligatorio
dcObject	*domainComponent* (partes del nombre del dominio)	suse	dc
organizationalUnit	*organizationalUnit* (unidad organizativa)	doc	ou
inetOrgPerson	*inetOrgPerson* (datos sobre personal para Internet/intranet)	Geeko Linux	sn y cn

En el ejemplo **??** en esta página puede ver un extracto de una instrucción de esquema con aclaraciones que le ayudarán a entender la sintaxis de nuevos esquemas.

Ejemplo 29.1: *Extracto de schema.core (numeración de líneas para facilitar la comprensión)*

```
#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) )
...
```

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.

29.3. Configuración de servidor con slapd.conf

Una vez que el sistema esté instalado existe 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. Las entradas precedidas del signo # se encuentran inactivas. Para activar dichas entradas basta con borrar el signo de comentario.

29.3.1. Instrucciones globales en slapd.conf

Ejemplo 29.2: *slapd.conf: instrucción Include para esquemas*

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/inetorgperson.schema
```

Con esta primera instrucción en `slapd.conf` se define el esquema utilizado para organizar el directorio LDAP (ver ejemplo **??** en esta página). 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.

Ejemplo 29.3: *slapd.conf: pidfile y argsfile*

```
pidfile /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args
```

Estos dos archivos contienen el número de identificación de proceso (PID o process id) y algunos argumentos con los que se iniciará el proceso slapd. En esta sección no es necesario realizar ningún cambio.

Ejemplo 29.4: *slapd.conf: Controles de acceso*

```
# Sample Access Control
#       Allow read access of root DSE
# Allow self write access
#       Allow authenticated users read access
#       Allow anonymous users to authenticate
# access to dn="" by * read
  access to * by self write
              by users read
              by anonymous auth
#
# if no access controls are present, the default is:
#       Allow read by all
#
# rootdn can always write!
```

El ejemplo **??** en esta página 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 estas. 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 **??** en esta página):

Cuadro 29.2: *Grupos de usuarios con acceso autorizado*

Identificador	Significado
*	todos los usuarios sin excepción
`anonymous`	usuarios no autenticados (”anónimos”)
`users`	usuarios autenticados
`self`	usuarios unidos al objeto destino
`dn.regex=<regex>`	todos los usuarios a los que puede aplicarse esta expresión regular

- ⟨*access*⟩ especifica el tipo de acceso. Aquí se distingue entre las posibilidades que aparecen en la tabla **??** en esta página:

Cuadro 29.3: *Tipos de acceso*

Identificador	Significado
`none`	acceso prohibido
`auth`	para contactar con el servidor
`compare`	para accesos comparables a objetos
`search`	para utilizar filtros de búsqueda
`read`	permiso de lectura
`write`	permiso de escritura

`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, este obtiene autorización. Si por

el contrario el cliente solicita más permisos que los concedidos en las reglas, el acceso será denegado.

El ejemplo **??** en esta página contiene un ejemplo muy de un sencillo control de acceso que puede configurarse de la forma deseada utilizando expresiones regulares.

Ejemplo 29.5: *slapd.conf: Ejemplo de control de acceso*

```
access to  dn.regex="ou=([^,]+),dc=suse,dc=de"
   by dn.regex="cn=administrator,ou=$1,dc=suse,dc=de" write
   by user read
   by * none
```

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.

Sugerencia

Definición de reglas Access

Si no es posible aplicar ninguna regla `access to` o instrucción `by`, 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.

Sugerencia

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 (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`.

29.3.2. Instrucciones para bases de datos en slapd.conf

Ejemplo 29.6: *slapd.conf: Instrucciones para bases de datos*

```
database            ldbm
suffix              "dc=suse,dc=de"
rootdn              "cn=admin,dc=suse,dc=de"
# Cleartext passwords, especially for the rootdn, should
# be avoided. See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw secret
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700 recommended.
directory /var/lib/ldap
# Indices to maintain
index objectClass eq
```

En la primera línea de esta sección (ver ejemplo **??** en esta página) 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 estas en lugar de las reglas `Access` globales.

29.3.3. 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 la sección **??** en esta página), puede iniciar el servidor LDAP como usuario `root` introduciendo el 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 la sección ?? en esta página) o bien crear directamente los enlaces correspondientes en los scripts de inicio y final por medio de `insserv` en la línea de comandos (ver sección **??** en esta página).

29.4. 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.

29.4.1. Introducir datos en el directorio LDAP

Como condición previa para la introducción de nuevas entradas, la configuración del servidor LDAP en `/etc/openldap/lsapd.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 (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 ?? en esta página podría presentar el siguiente aspecto (ver ejemplo **??** en esta página):

Ejemplo 29.7: *Ejemplo de archivo LDIF*

```
# 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
```

Importante

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. Le recomendamos que emplee un editor que soporte UTF-8 tal como Kate o las versiones más recientes de Emacs. Si se hubiera cambiado la codificación en su sistema, tiene que renunciar a la introducción de caracteres especiales o usar `recode` para convertir el texto a UTF-8.

Importante

Guarde el archivo como `.ldif` y páselo al servidor con el siguiente comando:

```
ldapadd -x -D <dn of the administrator> -W -f <file>.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 el ejemplo **??** en esta página de `ldapadd`:

Ejemplo 29.8: *ldapadd de ejemplo.ldif*

```
ldapadd -x -D cn=admin,dc=suse,dc=de -W -f example.ldif

Enter LDAP password:
adding new entry "dc=suse,dc=de"
adding new entry "ou=devel,dc=suse,dc=de"
adding new entry "ou=doc,dc=suse,dc=de"
adding new entry "ou=it,dc=suse,dc=de"
```

Los datos de usuario de los empleados de cada uno de los departamentos pueden introducirse en archivos LDIF adicionales. Por medio del siguiente ejemplo `tux.ldif` (ver ejemplo **??** en esta página), el empleado `Tux` es añadido al nuevo directorio LDAP:

Ejemplo 29.9: *Archivo LDIF para Tux*

```
# El empleado Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
objectClass: inetOrgPerson
cn: Tux Linux
givenName: Tux
sn: Linux
mail: tux@suse.de
uid: tux
telephoneNumber: +34 123 4567-8
```

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.

29.4.2. 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 el ejemplo **??** en esta página.

Ejemplo 29.10: *Archivo LDIF tux.ldif modificado*

```
# El empleado Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
changetype: modify
replace: telephoneNumber
telephoneNumber: +34 123 4567-10
```

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:

1. Ejecute `ldapmodify` e introduzca su contraseña:

   ```
   ldapmodify -x -D cn=admin,dc=suse,dc=de -W

   Enter LDAP password:
   ```

2. 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 (ldapmodify(1)).

29.4.3. 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 (ldapsearch(1)).

29.4.4. 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
```

29.5. El cliente LDAP de YaST

YaST soporta la gestión de usuarios vía LDAP. Para activarlo entre al módulo 'Servicios de red' → 'Cliente LDAP'. YaST instala y configura automáticamente las adaptaciones de LDAP para PAM y NSS tal como se explica en las líneas inferiores.

29.5.1. Procedimiento general

Para entender la función del módulo de cliente 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 login 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 ejemplo **??** en esta página).

Ejemplo 29.11: *pam_unix2.conf adaptado para LDAP*

```
auth:           use_ldap nullok
account:        use_ldap
password:       use_ldap nullok
session:        none
```

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` puede adaptar 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 **??** en esta página. El archivo `nsswitch.conf` ha de contener las siguientes líneas para la administración y autenticación de usuarios por medio de LDAP (ver ejemplo **??** en esta página):

Ejemplo 29.12: *Archivo nsswitch.conf adaptado*

```
passwd: compat
group: compat

passwd_compat: ldap
group_compat: ldap
```

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 el servidor LDAP. Pruebe este mecanismo ejecutando el comando `getent passwd` para leer, por ejemplo, el contenido de la base de datos de usuarios. En el resultado deberían

mostrarse tanto los usuarios locales de su sistema como los usuarios creados en el servidor LDAP.

Para evitar que los usuarios normales gestionados con LDAP entren mediante `ssh` o `login` al servidor, hay que añadir una línea a los archivos `/etc/passwd` y `/etc/group`. Al archivo `/etc/passwd` se le debe añadir la línea `+:::::::/sbin/nologin` y a `/etc/group` la línea `+:::`.

29.5.2. Configuración del cliente LDAP

Una vez que YaST ha adaptado los archivos `nss_ldap` y `pam_ldap` así como `/etc/passwd` y `/etc/group`, puede comenzar con el auténtico proceso de configuración en la primera máscara de YaST. Consulte la figura **??** en esta página.

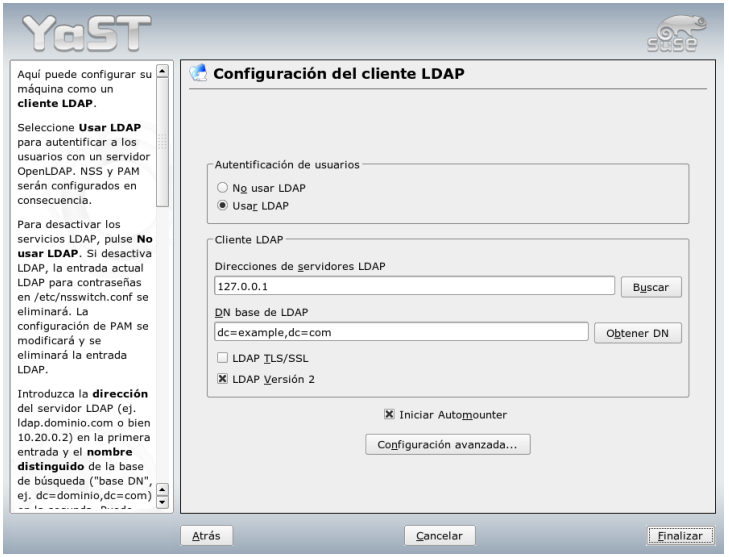

Figura 29.2: *YaST: Configuración del cliente LDAP*

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. Para montar directorios remotos sobre el sistema de archivos local, active la casilla 'Activar automounter'. Si desea poder modificar datos de forma activa en el servidor como administrador, pulse el botón 'Configuración avanzada'. Vea la figura **??** en esta página.

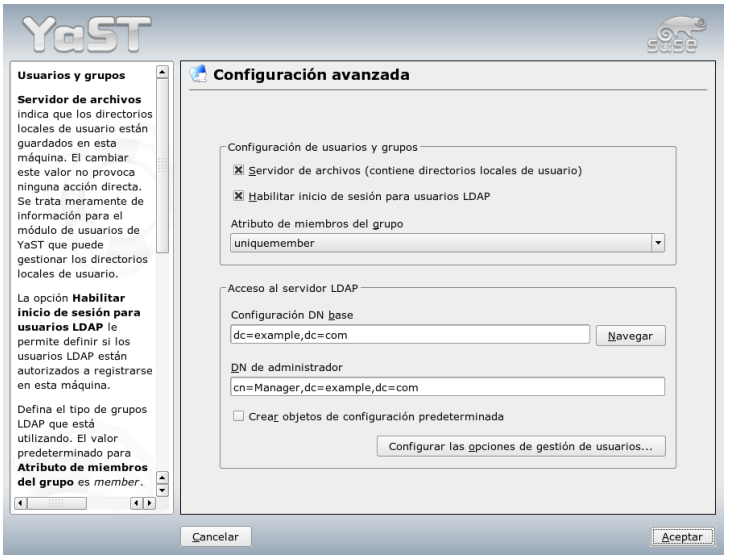

Figura 29.3: *YaST: configuración avanzada*

El siguiente diálogo está dividido en dos partes: La parte superior sirve para la configuración general de los usuarios y grupos. En la parte inferior se indican los datos de acceso al servidor LDAP. La configuración de usuarios y grupos se limita a las siguientes características:

Servidor de archivos Si su sistema un servidor de archivos que administra los directorios `/home` de los usuarios, active la casilla correspondiente para indicar al módulo de YaST cómo proceder con las carpetas de usuario en este sistema.

Permitir acceso a los usuarios de LDAP
Active esta casilla para permitir el login a los usuarios administrados por LDAP.

Atributo para miembro de grupo Determine el tipo de grupo LDAP a usar. Se puede elegir entre 'member' (estándar) y 'uniquemember'.

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 'DN de administrador'.

Pulse en 'Configurar gestión de usuarios' 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 de éste.

Importante

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.

Importante

El diálogo de la configuración de módulos le permite seleccionar y modificar módulos ya existentes, crear nuevos módulos o crear y editar plantillas (templates) para dichos módulos (ver figura **??** en esta página). 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'.

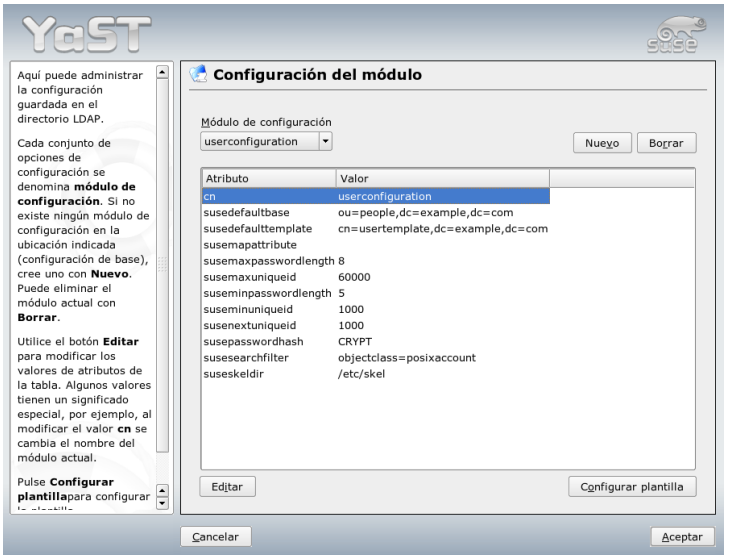

Figura 29.4: *YaST: Configuración de módulos*

Si desea complementar un módulo ya existente con un nuevo módulo, pulse el botón 'Nuevo' en el resumen de contenidos. Después introduzca en el diálogo emergente la clase de objeto del nuevo módulo (`suseuserconfiguration` o `susegroupconfiguration` 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 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 estos 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' (consulte la figura **??** en esta página). 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.

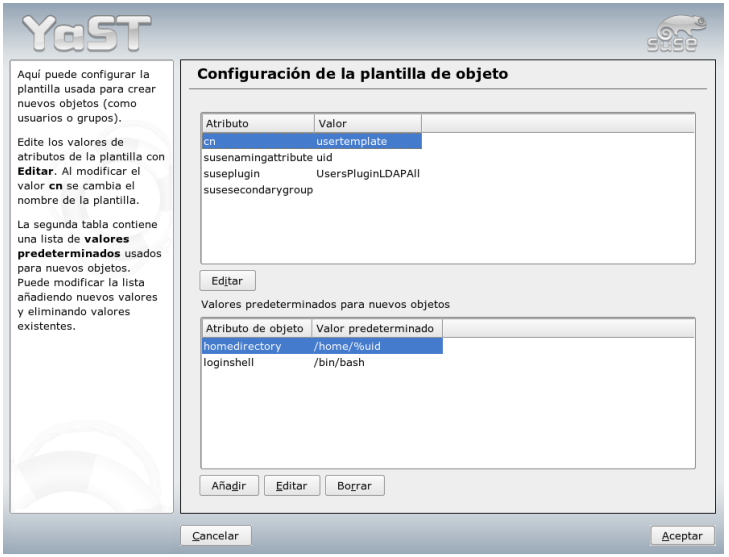

Figura 29.5: *YaST: Configuración de una plantilla de objeto*

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 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 `susedefaulttemplate` del módulo el DN de la plantilla modificada tal y como se ha descrito arriba.

Sugerencia

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`.

Sugerencia

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.

29.5.3. 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 la sección **??** en esta página. Si ya ha activado la utilización de LDAP, desde esta máscara pasa a otra donde se introducen los atributos específicos de LDAP (ver figura **??** en esta página). Seleccione uno tras otro los atributos cuyo valor desea modificar y pulse en 'Editar' para abrir los campos 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 se encuentra el botón 'Opciones de LDAP', que le permite aplicar filtros de búsqueda LDAP a los usuarios disponibles o con 'Config. LDAP de usuarios y grupos' acceder al módulo de configuración para usuarios y grupos LDAP.

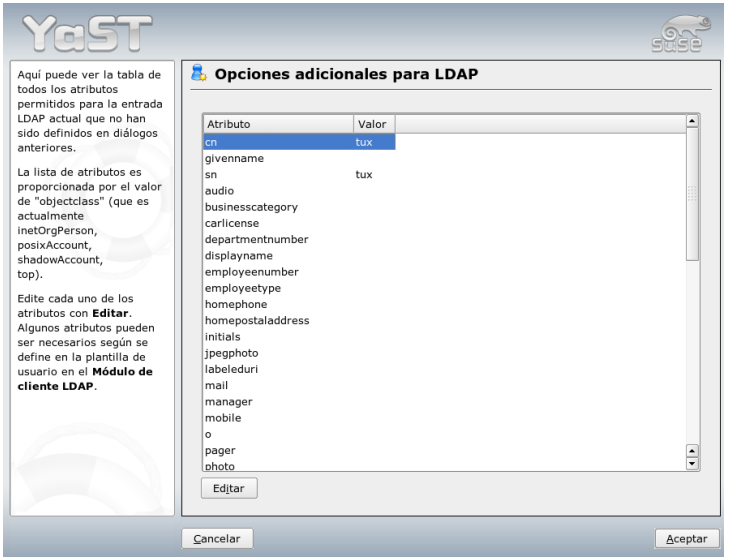

Figura 29.6: *YaST: opciones adicionales para LDAP*

29.6. 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 2.2 Administrator's Guide* (ver enlace más abajo).

La página web del proyecto OpenLDAP contiene abundante documentación en inglés para usuarios de LDAP tanto noveles como expertos:

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/admin22/quickstart.html` o bien en su sistema instalado en `/usr/share/doc/packages/openldap2/admin-guide/quickstart.html`

OpenLDAP 2.2 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/admin22/` 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 y Good: *Understanding and Deploying LDAP Directory Services*. Addison-Wesley, segunda edición, 2003. - (ISBN 0-672-32316-8)
- Hodges: *LDAP System Administration*. O'Reilly & Associates, 2003. - (ISBN 1-56592-491-6)

Los correspondientes RFCs (Request For Comments) 2251 a 2256 constituyen la obra de consulta definitiva sobre LDAP.

El servidor web Apache

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*.

Este capítulo está dedicado al servidor web Apache. Además de su instalación y configuración, en estas páginas se describen algunos de sus módulos así como las variantes para las máquinas virtuales.

30.1. Fundamentos

A continuación se describen a grandes rasgos los servidores web y los protocolos que utilizan.

30.1.1. 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).

30.1.2. 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 (HTTP). La versión actual de dicho protocolo (HTTP 1.1) está documentada en RFC 2068 y Update RFC 2616, los cuales se encuentran en la URL `http://www.w3.org`.

30.1.3. URLs

El cliente solicita una página al servidor a través de una URL. Por ejemplo: `http://www.novell.com/linux/suse/`. Una URL se compone de:

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.

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).

Recurso En este caso `index_us.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 (por ejemplo 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_us.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 `http://support.novell.com/linux/`.

La ruta al archivo es relativa con respecto al documento raíz o `DocumentRoot`, el cual puede modificarse en los archivos de configuración. El procedimiento correspondiente se describe en la sección DocumentRoot en esta página.

30.1.4. Reproducción automática de una página predeterminada

Indicar la página predeterminada 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 la sección DirectoryIndex en esta página. En este caso basta con especificar `http://www.suse.com` para que el servidor proporcione la página `http://www.novell.com/linux/suse/`.

30.2. Configuración del servidor HTTP con YaST

Apache puede configurarse con YaST rápida y fácilmente. No obstante, para poder implementarlo como servidor web es necesario un cierto nivel de conocimientos. Al seleccionar en el Centro de Control de YaST 'Servicios de red' → 'Servidor HTTP', se le preguntará si YaST debe instalar los paquetes que faltan. En caso de que esté todo instalado, accederá directamente al diálogo de configuración ('Configuración del servidor HTTP') .

En primer lugar, active el 'Servicio HTTP' y abra al mismo tiempo el cortafuegos ('Abrir cortafuegos en los puertos seleccionados') para los puertos necesarios (puerto 80). En la parte inferior de la ventana ('Resumen/Configuración') puede configurar algunas opciones para el propio servidor HTTP: 'Escuchar en' (la opción predeterminada es `Puerto 80`), 'Módulos', 'Ordenador predeterminado' y 'Ordenadores'. El botón 'Editar' le permite modificar la configuración para la opción seleccionada.

Compruebe en primer lugar el 'Ordenador predeterminado' y, si es necesario, modifique la configuración en función de sus necesidades. A continuación active los módulos deseados a través de la opción 'Módulos'. Además dispone de varios diálogos adicionales para la configuración detallada, en especial para la configuración de máquinas virtuales.

30.3. Los módulos de Apache

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.

Si se dispone de los conocimientos necesarios, Apache puede ser adaptado a los requisitos y necesidades del usuario mediante módulos escritos por él mismo. La sección **??** en esta página le ofrece indicaciones para obtener información adicional.

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 en Apache está muy acentuada. Aquí, el servidor se ocupa de un número muy reducido de tareas mientras que el resto se realiza a través de módulos. Esto se lleva a tal extremo que incluso el procesamiento de HTTP tiene lugar a través de módulos. Por lo tanto, Apache 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.

A continuación se describen algunas prestaciones muy útiles:

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 del 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 por ejemplo 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 (si se quiere acometer la tarea de adaptar el código JavaScript para cada navegador).

Flexibilidad en el tratamiento de errores
Al producirse un fallo (por ejemplo una página no está disponible), es posible reaccionar de forma flexible y responder convenientemente. El modo de respuesta puede configurarse de forma dinámica por ejemplo mediante CGI.

30.4. Threads

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", es decir, 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.

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 **??** en esta página). El tercer modo *perchild* aún se encuentra en una fase experimental y por eso (todavía) no se incluye en la instalación de SUSE LINUX.

30.5. Instalación

30.5.1. Selección de paquetes en YaST

Para solicitudes simples basta con instalar el paquete `apache2` (Apache 2). Instale además uno de los paquetes MPM (Multiprocessing Module) como `apache2-prefork` o `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".

30.5.2. Inicio de Apache

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 activarlo para 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 `apache2-example-pages` está instalado, podrá ver una página de prueba.

30.5.3. 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 `apache2-mod_perl` para Perl, el paquete `apache2-mod_php4` para PHP y el paquete `apache2-mod_python` para Python. El empleo de estos módulos se describe en la sección **??** en esta página.

30.5.4. Otros paquetes recomendados

De manera adicional se recomienda instalar la documentación (paquete `apache2-doc`). Después de instalar este paquete y activar el servidor (ver sección **??** en esta página) puede acceder directamente a la documentación 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 `apache2-devel`, así como las herramientas de desarrollo correspondientes, como por ejemplo las herramientas `apxs` que se describen en la sección **??** en esta página.

30.5.5. Instalación de módulos con apxs

`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, `apxs2` 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: `apxs2 -c -i -a mod_foo.c` Para ver opciones adicionales de `apxs2`, consulte las páginas del manual. Los módulos deben activarse mediante la entrada `APACHE_MODULES` en `/etc/sysconfig/apache2`, como se describe en la sección **??** en esta página.

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`.

30.6. Configuración

Una vez instalado Apache, sólo es necesario configurarlo si se tienen requisitos o necesidades especiales. La configuración de Apache puede llevarse a cabo mediante SuSEconfig y YaST o bien editando directamente el archivo `/etc/apache2/httpd.conf`.

30.6.1. Configuración con SuSEconfig

Las opciones que puede definir en `/etc/sysconfig/apache2`) son integradas en los archivos de configuración de Apache por medio de SuSEconfig. Las posibilidades de configuración incluidas bastan 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/apache2/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/apache2/httpd.conf` se sobreescriba al realizar una nueva instalación.

Módulos

Los módulos que han sido instalados con YaST se activan introduciendo el nombre del módulo en la lista de la variable `APACHE_MODULES`. 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.

30.6.2. Configuración manual

La edición del archivo de configuración `/etc/apache2/httpd.conf` permite realizar cambios que no son posibles mediante `/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 podría resultar algo bajo para una página muy visitada.

LoadModule

Las instrucciones `LoadModule` indican qué módulos se cargan. El orden de carga está definido a través de los mismos módulos. Asimismo, estas instrucciones especifican los archivos incluidos en el módulo.

Port

Define el puerto en el que Apache aguarda las solicitudes. Este 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.example.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. 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 esta página).

En `AllowOverride` se determina si la configuración definida en los archivos locales puede sobreescribir 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 para permitir todos los accesos y definir excepciones

deny all para denegar todos los accesos y definir 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 sobreescribir las opciones globales de configuración en los directorios proporcionados por Apache (ver la sección AllowOverride en esta página). 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 **??** en esta página) 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 esta página) 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` ⟨*nombre_archivo*⟩. 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 .shtml
AddHandler server-parsed .shtml
```

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/apache2/mod_userdir.conf` (el cual es cargado por `/etc/apache2/httpd.conf`).

```
<IfModule mod_userdir.c>
UserDir public_html
</IfModule>
```

30.7. Funcionamiento de Apache

Para mostrar sus propias páginas web (estáticas) con Apache basta con guardar los archivos en el directorio adecuado. En SUSE LINUX este 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. Estas pueden sobreescribirse sin problemas (o mejor aún, desinstalarse). Los scripts CGI propios se guardan en `/srv/www/cgi-bin`.

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`, etc.) se han solicitado y proporcionado. En caso de producirse fallos, encontrará la información correspondiente en el archivo `/var/log/apache2`.

30.8. Contenidos activos

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 por ejemplo 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.

Mientras los scripts CGI son activados por Apache (mediante el ID de usuario de su propietario), 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.

30.8.1. Server Side Includes

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 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 esta página.

30.8.2. Common Gateway Interface

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.

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 en la salida estándar (`stdout`).

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++.

En el caso más sencillo, Apache busca estos programas en un directorio concreto (`cgi-bin`). Este directorio puede definirse en el archivo de configuración, vea la sección **??** en esta página. Si es necesario, es posible especificar directorios adicionales que serán examinados por Apache 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.

30.8.3. 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 la entrada estándar (`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`.

30.8.4. Crear contenidos activos con módulos

Existen numerosos módulos que pueden utilizarse en Apache. El término "módulo" posee 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.

30.8.5. mod_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). 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 ?? en esta página). Las entradas necesarias para Apache en el archivo de configuración ya están incluidas, véase `/etc/apache2/mod_perl-startup.pl`. Puede obtener información adicional sobre `mod_perl` en `http://perl.apache.org/`.

Comparación entre 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:

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 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 con-

junto 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. `Apache::PerlRun` se comporta de manera similar a CGI.

30.8.6. 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/`. El paquete `mod_php4-core` ha de estar instalado necesariamente. Para Apache 2 se requiere además el paquete `apache2-mod_php4`.

30.8.7. 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. Ha de instalar el paquete `apache2-mod_python`.

Puede encontrar información adicional sobre este lenguaje en `http://www.python.org/` y sobre `mod_python` en `http://www.modpython.org/`

30.8.8. mod_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` 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/`.

30.9. 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. Existen 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.

30.9.1. 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. Esta 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/apache2/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.example.com
    DocumentRoot /srv/www/htdocs/example.com
    ServerAdmin webmaster@example.com
    ErrorLog /var/log/apache2/www.example.com-error_log
    CustomLog /var/log/apache2/www.example.com-access_log common
</VirtualHost>
```

```
<VirtualHost *>
    ServerName www.myothercompany.com
    DocumentRoot /srv/www/htdocs/myothercompany.com
    ServerAdmin webmaster@myothercompany.com
    ErrorLog /var/log/apache2/www.myothercompany.com-error_log
    CustomLog /var/log/apache2/www.myothercompany.com-access_log common
 </VirtualHost>
```

Para el dominio alojado originalmente por el servidor (`www.example.com`) debe crearse también una entrada `VirtualHost`. En este ejemplo el servidor aloja, además del dominio original, un dominio adicional (`www.myothercompany.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.

30.9.2. Máquinas virtuales en función de la dirección IP

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 ver la dirección IP utilizada por el ordenador. Puede añadir direcciones IP adicionales con el siguiente comando:

```
ip addr add 192.168.1.20/24 dev eth0
```

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.myothercompany.com
    DocumentRoot /srv/www/htdocs/myothercompany.com
    ServerAdmin webmaster@myothercompany.com
    ErrorLog /var/log/apache2/www.myothercompany.com-error_log
    CustomLog /var/log/apache2/www.myothercompany.com-access_log common
</VirtualHost>

<VirtualHost 192.168.1.21>
    ServerName www.anothercompany.com
    DocumentRoot /srv/www/htdocs/anothercompany.com
    ServerAdmin webmaster@anothercompany.com
    ErrorLog /var/log/apache2/www.anothercompany.com-error_log
    CustomLog /var/log/apache2/www.anothercompany.com-access_log common
</VirtualHost>
```

Aquí se introducen directivas `VirtualHost` sólo para los dominios adicionales, ya que el dominio original (`www.example.com`) se configura mediante las opciones correspondientes (`DocumentRoot`, etc.) fuera de los bloques `VirtualHost`.

30.9.3. 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
```

Para las otras dos instancias:

```
Listen 192.168.1.20:80
Listen 192.168.1.21:80
```

30.10. Seguridad

30.10.1. Riesgo mínimo

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.

30.10.2. 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 estos 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, por ejemplo `/srv/www/htdocs/miscellaneous`.

Publicar documentos del directorio local de usuario

Cuando los usuarios desean publicar en la red sus propios archivos es posible definir en el archivo de configuración un directorio en el directorio local de un usuario en el que este guarde sus archivos para la red (por ejemplo `~/public_html`). Esta posibilidad, activada por defecto en SUSE LINUX, se explica con más detalle en la sección UserDir en esta página.

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 tux.

30.10.3. 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 estos.

En la sección **??** en esta página se incluyen algunas fuentes de información sobre exploits y correcciones.

30.11. 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. A continuación le indicamos algunos de los pasos a seguir. 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/apache2/error_log`.

Se recomienda seguir los archivos de registro en una consola mientras se accede al servidor para ver cómo reacciona este en cada momento. Con este fin, ejecute en una consola el siguiente comando como `root`:

```
tail -f /var/log/apache2/*_log
```

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/`.

30.12. Información adicional

Apache es un servidor web de uso muy extendido. En consecuencia, existe una gran cantidad de información disponible y muchos sitios web con material de ayuda sobre este tema.

30.12.1. Apache

Apache dispone de abundante documentación que puede instalar como se describe en la sección ?? en esta página. 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`

30.12.2. CGI

Puede encontrar información adicional (en inglés) sobre CGI en:

- `http://apache.perl.org/`
- `http://perl.apache.org/`

- http://www.modperl.com/
- http://www.modperlcookbook.org/
- http://www.fastcgi.com/
- http://www.boutell.com/cgic/

30.12.3. Seguridad

La página http://www.novell.com/linux/security/securitysupport.html contiene los parches actuales para los paquetes de SUSE LINUX. 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.de o a security@apache.org.

30.12.4. Fuentes adicionales

En caso de problemas le recomendamos consultar la base de datos de soporte de SUSE http://portal.suse.com/sdb/en/index.html. 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.

Puede obtener información sobre la actualización de la versión 1.3 a la versión 2.0 en http://httpd.apache.org/docs-2.0/es/upgrading.html.

Sincronización de archivos

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 archivos se necesitan en todos los ordenadores. Lo ideal sería poder disponer siempre de todos los archivos en todos los ordenadores en su versión actual.

31.1. Software de sincronización de 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 archivos de red como NFS y guardar los archivos 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 archivos que necesite en el disco duro local. No obstante, cuando los archivos son editados no tarda en surgir el problema de la sincronización. Al modificar un archivo en un ordenador debe intentarse actualizar la copia de ese archivo 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 archivos resulta un proceso muy laborioso que requiere mucha atención por parte del usuario para no cometer fallos como, por ejemplo, sobreescribir un nuevo archivo 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 archivos 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 propósito de las breves descripciones que aparecen a continuación es simplemente dar al usuario una ligera idea sobre el funcionamiento de estos programas. En caso de querer aplicar estos programas, le recomendamos leer atentamente la documentación de los mismos.

31.1.1. Unison

En el caso de Unison no se trata de un sistema de archivos, sino que los archivos se guardan y editan normalmente de forma local. El programa Unison puede ejecutarse manualmente para sincronizar archivos. 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 archivos seleccionados.

La próxima vez que se ejecute, Unison reconoce qué archivos 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.

31.1.2. CVS

CVS se utiliza sobre todo para administrar versiones de textos fuente de programas y ofrece la posibilidad de guardar copias de archivos 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 archivos 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.

31.1.3. Subversion

A diferencia de CVS, que simplemente "evolucionó" a lo largo del tiempo, Subversion es un proyecto diseñado de forma consecuente para reemplazar a CVS y superarlo desde el punto de vista tecnológico.

Subversion sobrepasa en muchos detalles a su antecesor. Por razones históricas, CVS sólo gestiona archivos porque "desconoce" los directorios. En cambio, en Subversion los directorios tienen también un historial de versiones y se pueden copiar o cambiar de nombre del mismo modo que los archivos. Además es posible añadir metadatos a todo archivo o directorio sometido al control de versiones. A diferencia de CVS, Subversion permite un acceso transparente a través de la red mediante algunos protocolos como por ejemplo WebDAV (Web-based Distributed Authoring and Versioning). WebDAV amplía la funcionalidad del protocolo HTTP para permitir el acceso de escritura de colaboración para archivos en servidores web remotos.

Para el desarrollo de Subversion se utilizaron paquetes de software ya existentes. Por este motivo siempre se requiere el servidor web Apache con la extensión WebDAV para poder ejecutar Subversion.

31.1.4. 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 archivos 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 este ha de borrarse o si debe ser sincronizado. Se permite la sincronización tanto entre buzones sueltos como entre jerarquías de buzones.

31.1.5. rsync

Si no se requiere un control de versiones, la herramienta rsync es la opción ideal para sincronizar grandes árboles de archivos a través de conexiones de red lentas. rsync dispone de mecanismos sofisticados para transmitir exclusivamente los cambios en los archivos. No sólo funciona con archivos de texto, sino también con archivos binarios. rsync divide los archivos en bloques y calcula las sumas de control para reconocer las diferencias entre archivos.

El reconocimiento de los cambios en los archivos exige un gran esfuerzo. Por eso, los ordenadores cuyos datos se sincronizan han de ser lo suficientemente potentes. Conviene sobre todo no ahorrar en memoria RAM.

31.2. Criterios para la elección de programa

31.2.1. 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") comparen sus archivos. 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 Subversion, CVS y WebDAV. La alternativa consiste en que todos los ordenadores tengan los mismos derechos y comparen sus datos entre sí. Este es el planteamiento empleado por Unison. En realidad rsync trabaja en modo cliente servidor, pero cada cliente puede utilizarse a su vez como servidor.

31.2.2. Portabilidad

Subversion, CVS y Unison están disponibles para muchos otros sistemas operativos, como es el caso de otros Unix y Windows.

31.2.3. Interactivo o automático

La sincronización de datos en Subversion, CVS, WebDAV y Unison es iniciada por el usuario. Esto permite un mayor control sobre los archivos 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.

31.2.4. Conflictos: cuándo aparecen y cómo resolverlos

En Subversion o 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 Subversion o CVS se resuelven fácilmente.

Los conflictos en Unison se notifican al usuario y el archivo se puede entonces excluir de la sincronización. Por otra parte, los cambios no se fusionan tan fácilmente como en Subversion o CVS.

Subversion o CVS aceptan parcialmente los cambios también en caso de un conflicto. En cambio WebDAV sólo registra los cambios si no existe ningún conflicto en toda la modificación.

rsync no maneja ni resuelve conflictos. El usuario es quien tiene que preocuparse de no sobreescribir por equivocación archivos y de resolver manualmente todos los conflictos que se presenten. Para controlarlo puede utilizar adicionalmente un sistema de control de versiones como RCS.

31.2.5. Seleccionar y añadir archivos

En su configuración predeterminada, Unison sincroniza un árbol completo de directorios. Los nuevos archivos presentes en el árbol se incorporan automáticamente a la sincronización.

En el caso de Subversion o CVS es necesario añadir explícitamente nuevos directorios y archivos por medio de `svn add` y `cvsadd` respectivamente. La consecuencia es un mayor control sobre los archivos que van a formar parte de la

sincronización. Por otra parte, los nuevos archivos tienden a olvidarse; sobre todo si debido al número de archivos se ignora el signo '?' que aparece en la salida de `svn update`, `svn status` y `cvs update` respectivamente.

31.2.6. Historia

Como función adicional, Subversion o CVS permiten reconstruir las versiones anteriores de los archivos. Cada vez que se realiza un cambio es posible añadir una pequeña nota y posteriormente reproducir el desarrollo del archivo basándose en el contenido y en los comentarios. Esto resulta de gran utilidad en el caso de tesis o textos de programas.

31.2.7. Volumen de datos y requisitos de espacio en el disco duro

En cada uno de los ordenadores participantes se necesita espacio suficiente en el disco duro para todos los datos distribuidos. En el caso de Subversion o CVS se necesita además espacio adicional para la base de datos (repository) en el servidor. Allí también se guarda la historia de los archivos, por lo que los requisitos de espacio son mucho mayores que el espacio necesario en sí. En el caso de archivos 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 archivos binarios, el espacio requerido aumenta en el orden del tamaño del archivo con cada cambio que se produce.

31.2.8. GUI

Unison está equipado con una interfaz gráfica que muestra la sincronización sugerida por Unison. Se puede aceptar esta propuesta o bien excluir archivos 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 Subversion o 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 o Subversion. A menudo, el uso de estos frontales simplifica en gran medida la resolución de conflictos.

31.2.9. Facilidad de uso

Unison y rsync son muy fáciles de usar y resultan adecuados también para usuarios principiantes. El manejo de Subversion y 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 `cvs update` o `svn update`. Una vez hecho esto, los datos deben volver a enviarse al repositorio con `cvs commit` o `svn commit`. Siempre que se respeten estos procesos, el uso de CVS o Subversion es muy sencillo incluso para principiantes.

31.2.10. 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, rsync o Subversion pueden utilizarse a través de 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. Subversion ofrece automáticamente los mecanismos de seguridad necesarios porque utiliza Apache.

31.2.11. 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 fallos del usuario (como por ejemplo la eliminación accidental de un archivo). Aunque Subversion aún no se utiliza con tanta frecuencia como CVS, ya es usado en el área productiva (por ejemplo el mismo proyecto Subversion lo utiliza).

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 archivo durante la sincronización, no hay vuelta atrás. Lo mismo pasa con rsync.

Cuadro 31.1: *Prestaciones de las herramientas de sincronización de datos: -- = muy malo, - = malo o no disponible, o = regular, + = bueno, ++ = muy bueno, x = disponible*

	Unison	**CVS/subv.**	**rsync**	**mailsync**
Cliente/servidor	igualdad	C-S/C-S	C-S	igualdad
Portabilidad	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x
Interacción	x	x/x	x	-
Velocidad	-	o/+	+	+
Conflictos	o	++/++	o	+
selecc.fich.	directorio	selecc./fich., direct.	directorio	buzón
Historia	-	x/x	-	-
Esp. disco	o	--	o	+
GUI	+	o/o	-	-
Dificultad	+	o/o	+	o
Ataques	+(ssh)	+/+(ssh)	+(ssh)	+(SSL)
Pérdida datos	+	++/++	+	+

31.3. Introducción a Unison

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.

31.3.1. 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 la sección **??** en esta página).

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.

31.3.2. 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:

Cliente:	`/home/tux/dir1`
Servidor:	`/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 archivos y directorios individuales. La flecha en la columna Action define el sentido de la transmisión. Un signo de interrogación 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`.

Ejemplo 31.1: *El archivo ~/.unison/example.prefs*

```
root=/home/tux/dir1
root=ssh://wilber@server//homes/wilber/dir2
batch=true
```

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` Para iniciar la sincronización, basta con introducir este archivo como argumento en la línea de comandos: `unison example.prefs`

31.3.3. 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 `unison` de SUSE.

31.4. Introducción a CVS

CVS se recomienda para tareas de sincronización en el caso de archivos 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 archivo se almacenan permanentemente en el servidor CVS. Además, en estos casos no se utilizan todas las prestaciones de CVS. El uso de CVS para sincronizar datos sólo es posible cuando todas las estaciones de trabajo tiene acceso al mismo servidor.

31.4.1. Configuración del servidor CVS

El *servidor* es la máquina en la que están situados todos los archivos válidos, incluyendo la versión actual de todos los archivos. 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. Si el usuario es conocido en el servidor como `tux` y 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 `cvs 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:

```
cvs import synchome tux wilber
```

Nota: Muchos comandos de CVS requieren un comentario. Para ello, CVS inicia un editor (aquel 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:

```
cvs import -m 'es una prueba' synchome tux wilber
```

31.4.2. Manejo de CVS

A partir de este momento, el repositorio de la sincronización puede extraerse desde cualquier ordenador con `cvs 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 comando `cvs commit`.

Este comando transmite por defecto todos los archivos (incluyendo subdirectorios) al servidor. Si sólo se quieren transmitir determinados archivos o directorios, estos deben especificarse en el comando por ejemplo del siguiente modo: `cvs commit archivo1 directorio1`. Antes de ser transmitidos al servidor, los nuevos archivos o directorios han de declararse parte integrante de CVS con `cvs add archivo1 directorio1` y a continuación enviarse al servidor con `cvs commit archivo1 directorio1`.

Si se cambia de estación 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 esa misma estación de trabajo.

Para iniciar la sincronización con el servidor se utiliza `cvs update`. Si desea actualizar archivos o directorios determinados, especifíquelos con `cvs update archivo1 directorio1`. Si se quieren ver las diferencias entre las versiones almacenadas en el servidor, se utiliza el comando `cvs diff` o bien `cvs diff archivo1 directorio1`. De manera alternativa, se puede utilizar el comando `cvs -nq update` para mostrar los archivos afectados por una actualización.

Durante el proceso de actualización se muestran, entre otros, los siguientes símbolos indicadores de estado:

U La versión local ha sido actualizada. El proceso de actualización afecta a todos los archivos proporcionados por el servidor y que no están presentes en el sistema local.

M La versión local ha sido modificada. Si existían cambios en el servidor, es posible fusionar las diferencias en la copia local.

P La versión local ha sido parcheada. Es decir, CVS ha intentado fusionar la versión en el servidor CVS con la versión local.

C Existe un conflicto entre el archivo local y la versión actual del repositorio.

? Este archivo no se encuentra en CVS.

El estado `M` señaliza los archivos modificados localmente. En este caso puede enviar la copia local con los cambios al servidor o bien, si prefiere prescindir de los cambios y adoptar la versión del servidor, puede eliminarse la copia local y llevar a cabo una actualización, con lo que el archivo que falta se obtiene del servidor. Si sucede que diversos usuarios realizan cambios en idéntico pasaje de un mismo archivo, CVS no es capaz de decidir qué versión ha de ser utilizada. En este caso, la actualización se señalaría con el símbolo `C` de conflicto.

En este caso examine los signos de conflicto (Â»> y Â«<) en el archivo para optar por una de las dos versiones. Si esta labor resulta demasiado complicada, siempre puede abandonar los cambios, borrar el archivo local y ejecutar `cvs up` para obtener la versión actual del servidor.

31.4.3. 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/
```

31.5. Introducción a Subversion

Subversion es un sistema de control de versiones de código abierto y es considerado el sucesor de CVS. Por eso ciertas características de CVS ya presentadas son iguales en Subversion. Es muy indicado para disfrutar de las ventajas de CVS sin ninguno de sus inconvenientes. Muchas de sus prestaciones ya fueron presentadas en la sección **??** en esta página.

31.5.1. Instalación de un servidor Subversion

Establecer un repositorio en un servidor es relativamente simple. Subversion dispone para ello de una herramienta de administración especial llamada `svnadmin`. El repositorio nuevo se crea con:

```
svnadmin create /ruta/al/repositorio
```

La ayuda muestra opciones adicionales: `svnadmin help`. A diferencia de CVS, Subversion no está basado en RCS sino que utiliza la base de datos de Berkeley. El repositorio *no* se puede encontrar sobre sistemas de archivos remotos como NFS, AFS o Windows SMB, porque la base de datos necesita mecanismos de bloqueo del tipo POSIX. Estos mecanismos no existen en los sistemas de archivos mencionados.

El comando `svnlook` sirve para ver el contenido de un repositorio existente:

```
svnlook info /ruta/al/repositorio
```

El servidor debe ser configurado de tal forma que distintos usuarios puedan acceder al repositorio. Utilice el servidor web Apache o bien el servidor propio de Subversion llamado `svnserve`. Una vez que `svnserve` se está ejecutando, las URL `svn://` o `svn+ssh://` permiten el acceso directo al repositorio. En el archivo `/etc/svnserve.conf` puede introducir a los usuarios que tienen que autentificarse en el momento de usar el comando `svn`.

La decisión a favor o en contra de un determinado sistema de control de versiones depende de muchos factores. Para más información consulte la sección **??** en esta página.

31.5.2. Manejo de Subversion

El acceso a un repositorio de Subversion se realiza con el comando `svn` (similar a `cvs`). Si el servidor está correctamente configurado (con su correspondiente repositorio), se puede mostrar el contenido en cada cliente mediante:

```
svn list http://svn.example.com/ruta/al/proyecto
```

o

```
svn list svn://svn.example.com/ruta/al/proyecto
```

El comando `svn checkout` sirve para guardar un proyecto existente en el directorio actual (check out):

```
svn checkout http://svn.example.com/ruta/al/proyecto NombreProyecto
```

Realizando el "checkout" se crea en el cliente un subdirectorio nuevo denominado `NombreProyecto`. Dentro de este puede realizar cualquier modificación (añadir, copiar, renombrar, borrar):

```
svn add file
svn copy oldfile newfile
svn move oldfile newfile
svn delete file
```

Se puede aplicar cada uno de estos comandos para archivos y para directorios. Además Subversion es capaz de guardar properties (propiedades) de un archivo o directorio:

```
svn propset license GPL foo.txt
```

El comando anterior deja la propiedad `license` del archivo `foo.txt` en el valor `GPL`. Mediante `svn proplist` se puede ver las propiedades:

```
svn proplist --verbose foo.txt
Properties on 'foo.txt':
  license : GPL
```

Los cambios se publican, es decir, se guardan en el servidor con el comando `svn commit`. Otros usuarios que quieran disponer de los cambios realizados por Ud. en sus propios directorios, tienen que sincronizarse con el servidor mediante `svn update`.

A diferencia de CVS, es posible mostrar el estado de un directorio de trabajo de Subversion *sin* acceder al repositorio por medio de `svn status`. Los cambios locales se muestran en cinco columnas, siendo la primera la más importante:

" Sin cambios.

'A' El objeto se añade.

'D' El objeto se borra.

'M' El objeto ha sido modificado.

'C' El objeto está en conflicto.

'I' El objeto se ignora.

'?' El objeto no está sometido al control de versiones.

'!' Objeto desaparecido. Esta marca aparece cuando el objeto ha sido borrado o movido sin el comando `svn`.

'~' El objeto se ha administrado como archivo pero ha sido reemplazado por un directorio (o un directorio reemplazado por un archivo).

La segunda columna muestra las propiedades (properties). Para el significado de las demás columnas, consulte el libro de Subversion.

Con `svn help` puede acceder a la ayuda rápida para obtener una descripción de un parámetro de un comando:

```
svn help proplist
proplist (plist, pl): List all properties on files, dirs, or revisions.
usage: 1. proplist [PATH...]
       2. proplist --revprop -r REV [URL]

  1. Lists versioned props in working copy.
  2. Lists unversioned remote props on repos revision.
...
```

31.5.3. Información adicional

El punto de partida es la página web de Subversion en `http://subversion.tigris.org`. Después de instalar el paquete `subversion-doc`, un libro muy recomendable (en inglés) se encuentra en el directorio `file:///usr/share/doc/packages/subversion/html/book.html`. También puede consultarlo en línea en `http://svnbook.red-bean.com/svnbook/index.html`

31.6. Introducción a rsync

rsync resulta ideal para la transferencia periódica de grandes cantidades de datos que no varían mucho. Esto suele ser el caso en las copias de seguridad. Otra aplicación son los denominados staging server. Estos contienen el árbol original y completo de un servidor web. Este árbol se copia periódicamente al servidor web verdadero en la "DMZ".

31.6.1. Configuración y manejo

Existen dos modos de operación para rsync. Por una parte, rsync sirve para archivar y copiar archivos. Esto sólo requiere un shell remoto en el ordenador destino como por ejemplo ssh. Por otra parte, rsync puede actuar como `daemon` y ofrecer directorios en la red.

El uso básico de rsync no requiere ninguna configuración especial. Por ejemplo, resulta muy sencillo replicar un directorio completo de un ordenador a otro. El siguiente comando sirve para crear una copia de seguridad del directorio personal de tux en el servidor de copias de seguridad sol:

```
rsync -baz -e ssh /home/tux/ tux@sol:backup
```

Para volver a copiar el directorio al ordenador local se utiliza el comando:

```
rsync -az -e ssh tux@sol:backup /home/tux/
```

Hasta este punto el uso de rsync casi no difiere de un programa de copia como scp.

Para poder utilizar todas sus prestaciones, rsync ha de utilizarse en modo "rsync". Para ello se arranca el daemon rsyncd en uno de los ordenadores. Este daemon se configura con el archivo `/etc/rsyncd.conf`. Por ejemplo, para dar acceso vía rsync al directorio `/srv/ftp`, se puede utilizar el siguiente archivo de configuración:

```
gid = nobody
uid = nobody
read only = true
use chroot = no
transfer logging = true
log format = %h %o %f %l %b
log file = /var/log/rsyncd.log

[FTP]
        path = /srv/ftp
        comment = An Example
```

Inicie a continuación rsyncd con `rcrsyncd start`. Para iniciar rsyncd automáticamente al arrancar el ordenador, se puede activar este servicio en el editor de niveles de ejecución de YaST o bien introducir el comando `insserv rsyncd`. Una alternativa es el inicio de rsyncd desde xinetd, pero esto sólo se recomienda para servidores que no utilizan rsyncd con mucha frecuencia.

El ejemplo también crea un archivo de registro con todas las conexiones. Dicho archivo se encuentra en `/var/log/rsyncd.log`.

La transferencia desde un ordenador cliente puede comprobarse mediante:

```
rsync -avz sol::FTP
```

Este comando produce una lista de todos los archivos que se encuentran dentro del directorio `/srv/ftp` en el servidor. Esta consulta aparece también en el archivo de registro `/var/log/?syncd.log`. Para iniciar la transferencia hace falta indicar un directorio destino que puede ser "." si se trata del directorio actual, es decir:

```
rsync -avz sol::FTP .
```

Con su configuración predeterminada, rsync no borra archivos durante la sincronización. Para lograr este efecto es preciso utilizar la opción adicional `--delete`. Usando la opción `--update` los archivos con fecha reciente no son reemplazados por los archivos con fecha anterior. Los posibles conflictos que aparezcan se han de resolver manualmente.

31.6.2. Información adicional

Las páginas del manual `man rsync` y `man rsyncd.conf` informan sobre el uso de rsync. Puede obtener documentación técnica sobre el funcionamiento de rsync en `/usr/share/doc/packages/rsync/tech_report.ps` La página web del proyecto rsync contiene la información más actual rsync: `http://rsync.samba.org`.

31.7. Introducción a mailsync

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.

31.7.1. 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 archivo `~/.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 el comando `mailsync -m saved-messages`, se mostrará un índice de todos los mensajes guardados en saved-messages. Otra posible definición sería:

```
store localdir {
pat     Mail/*
prefix  Mail/
}
```

En este caso, la ejecución de `mailsync -m localdir` produce una lista de todos los mensajes almacenados en las carpetas de `Mail/`. Por su parte, 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}
```

Este prefijo se explica posteriormente.

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 archivo 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` (presuponiendo 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 archivo `msinfo`) será transmitido a esa parte.

- Si un mensaje existe sólo en una parte y es antiguo (ya está registrado en el archivo `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.

31.7.2. Posibles problemas

En caso de pérdida de datos, el procedimiento más seguro consiste en borrar el archivo 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 este 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`.

31.7.3. Información adicional

Puede encontrar más información en el `README` incluido en el paquete mailsync en `/usr/share/doc/packages/mailsync/`. En este contexto, el RFC 2076 "Common Internet Message Headers" también contiene información de gran interés.

Samba

Samba permite implementar un equipo Unix como servidor de archivos e impresión para máquinas DOS, Windows y OS/2. Este capítulo presenta los fundamentos de la configuración de Samba y describe los módulos de YaST que le ayudarán a configurar Samba en la red.

Samba se ha convertido en un producto muy completo, por lo que aquí nos centramos exclusivamente en su funcionalidad. No obstante, puede obtener información adicional en la documentación en formato digital incluida en la distribución. Dicha documentación consta por un lado de las páginas del manual (a las que puede acceder, por ejemplo, introduciendo `apropos samba` en la línea de comandos) y, por otro lado, de documentos y ejemplos que se encuentran en `/usr/share/doc/packages/samba` siempre que haya instalado Samba en el sistema. El subdirectorio `examples` contiene un ejemplo de configuración comentado, `smb.conf.SuSE`.

El paquete `samba` se encuentra disponible en la versión 3. Entre las novedades de esta nueva versión cabe destacar:

- Soporte de Active Directory.
- Soporte Unicode considerablemente mejorado.
- Mecanismos internos de autentificación completamente revisados.
- Soporte mejorado del sistema de impresión de Windows 200x y XP.
- Configuración como servidor miembro en dominios Active Directory.
- Adopción de dominios NT4 para posibilitar la migración de un dominio NT4 a un dominio Samba.

Sugerencia

Migración a Samba 3

A la hora de migrar de la versión 2.x a la versión 3 de Samba, debe tener en cuenta algunas peculiaridades. La información correspondiente se ha recogido en un nuevo capítulo de la colección de HOWTOs de Samba. Una vez instalado el paquete `samba-doc`, encontrará el HOWTO en `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

Sugerencia

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 es una interfaz para programas de aplicación (Application Program Interface, API), que se diseñó para la comunicación entre ordenadores. Entre otros, ofrece un servicio de nombres (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 otro. 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 esta es la opción por defecto.

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 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 recursos compartidos o "shares". Un share es un directorio en el servidor con todos los subdirectorios. Este 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.

32.1. 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`, Este 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 `[global]`, lo que se recomienda por motivos de claridad.

32.1.1. La sección global

Los siguientes parámetros de la sección `global` deben ser definidos de acuerdo a la configuración de la red a fin de que otras máquinas puedan acceder al servidor Samba en una red Windows por medio de SMB.

workgroup = TUX-NET Esta línea asigna el servidor Samba a un grupo de trabajo. Sustituya `TUX-NET` por un grupo de trabajo de su entorno de red. El servidor Samba aparece aquí con el nombre DNS a no ser que dicho nombre haya sido asignado a otro máquina de la red. Si el nombre DNS no está disponible, es posible definir el nombre del servidor mediante `netbiosname=MINOMBRE`. Puede obtener información adicional sobre este parámetro con `man smb.conf`.

os level = 2 En función de este parámetro el servidor Samba decide si quiere convertirse en un LMB (Local Master Browser) para su grupo de trabajo. Seleccione un valor bajo para que la red de Windows existente 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` disponibles en el subdirectorio `textdocs` de la documentación del paquete.

Si en la red no existe ningún otro servidor SMB (como un servidor Windows NT o 2000) y desea que el servidor Samba mantenga una lista de los sistemas disponibles en la red local, incremente el valor de `os level` (por ejemplo 65) para que el servidor Samba sea elegido LMB para la red local.

A la hora de modificar este valor, tenga en cuenta cómo puede afectar el cambio al funcionamiento de una red Windows ya existente. Pruebe los cambios primero en una red aislada o en momentos poco 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`. En este parámetro se debe introducir la dirección IP del servidor WINS.

Si las máquinas Windows están conectadas a subredes separadas y han de ser visibles entre sí, necesita un servidor WINS. Para convertir su servidor Samba en un servidor WINS, defina la opción `wins support = Yes`. Asegúrese de que este parámetro se activa exclusivamente en un servidor Samba. Las opciones `wins server` y `wins support` no pueden estar nunca activas simultáneamente en smb.conf.

32.1.2. 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] 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.

Ejemplo 32.1: *Acceso al CD-ROM*

```
;[cdrom]
;       comment = Linux CD-ROM
;       path = /media/cdrom
;       locking = No
```

`[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 está disponible 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]`.

\mbox{[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.

Ejemplo 32.2: *Recurso compartido homes*

```
[homes]
        comment = Home Directories
        valid users = %S
        browseable = No
        read only = No
        create mask = 0640
        directory mask = 0750
```

[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]` este 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 `writeable = 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.

32.1.3. 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: (security = share)
En este caso cada share tiene una contraseña fija. Cada persona que conoce la contraseña tiene acceso al share.

User Level Security: (security = user) 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 autentificación, el servidor puede otorgar derechos de acceso a los distintos shares exportados en función del nombre de usuario.

Server Level Security: (security = server)
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 autentificación. Esta configuración requiere de un parámetro adicional (`password server =`).

La decisión sobre el tipo de autentificación es algo que afecta a todo el servidor. No es posible exportar unos recursos compartidos de la configuración de un servidor en modalidad "Share Level Security" y otros en "User Level Security". No obstante, es posible ejecutar en un sistema un servidor Samba propio para cada dirección IP configurada.

La colección de HOWTOs de Samba contiene más información al respecto. En el caso de un sistema con varios servidores, tenga en cuenta los parámetros `interfaces` y `bind interfaces only`.

Sugerencia

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 archivo `/etc/xinetd.d/samba` y `/etc/services`. Para ello debe modificar la línea `disable = no` en el archivo `/etc/xinetd.d/samba`. Puede obtener información adicional acerca de este programa en la página del manual de swat.

Sugerencia

32.2. Samba como servidor de dominio

En redes con clientes mayoritariamente Windows, a menudo es preferible que los usuarios sólo puedan acceder a los recursos con su nombre de usuario y una contraseña, lo que puede realizarse por medio de un servidor Samba. En una red basada en Windows, un servidor de Windows NT se encarga de esta tarea cuando está configurado como Primary Domain Controller (PDC). En el siguiente ejemplo **??** en esta página se muestran las entradas que es necesario realizar en la sección `[global]` de `smb.conf` en el caso de Samba.

Ejemplo 32.3: *Sección global de smb.conf*

```
[global]
        workgroup = TUX-NET
        domain logons = Yes
        domain master = Yes
```

Para usar contraseñas codificadas para la autentificación, 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 `[globals]`. Este valor ya está predeterminado a partir de la versión 3 de samba. Además, las cuentas de los usuarios y las contraseñas se deben codificar en una forma que Windows

entienda. Utilice para ello 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:

Ejemplo 32.4: *Creación de una cuenta de ordenador*

```
useradd nombre_ordenador\$
smbpasswd -a -m nombre_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 `/usr/share/doc/packages/samba/examples/smb.conf.SuSE` se encuentran configuraciones que automatizan este trabajo.

Ejemplo 32.5: *Creación automática de una cuenta de ordenador*

```
add machine script = /usr/sbin/useradd -g nogroup \
    -c "NT Machine Account" -s /bin/false %m\$
```

Para que Samba pueda ejecutar correctamente este script, se requiere un usuario Samba con permisos de administrador. Con este fin, seleccione un usuario y añádalo al grupo `ntadmin`. A continuación puede añadir todos los usuarios de este grupo Linux al grupo ”Domain Admins” con el siguiente comando:

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

Puede obtener información adicional en el capítulo 12 de la colección de HOWTOs de Samba: `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

Figura 32.1: *Configuración de Samba: inicio*

32.3. Configuración del servidor Samba con YaST

Inicie la configuración del servidor seleccionando el grupo de trabajo o dominio del que se ocupará el servidor Samba. Puede asignar al servidor un grupo de trabajo/dominio ya existente (los que se encuentren serán mostrados en el apartado 'Nombre de grupo de trabajo o dominio') o bien crear un grupo de trabajo nuevo. A continuación debe especificar si el servidor ha de actuar como controlador de dominio primario (PDC) o bien como controlador de dominio de reserva (BDC).

Active Samba en el menú de 'Inicio' (figura **??** en esta página). Utilice los menús 'Puerto abierto en el cortafuegos' y 'Detalles del cortafuegos' para configurar el cortafuegos en el servidor de forma que los puertos para los servicios `netbios-ns`, `netbios-dgm`, `netbios-ssn` y `microsoft-ds` estén abiertos en todas las interfaces externas e internas, garantizando un funcionamiento sin problemas del servidor Samba.

El menú 'Recursos compartidos' (figura **??** en esta página) le permite definir qué

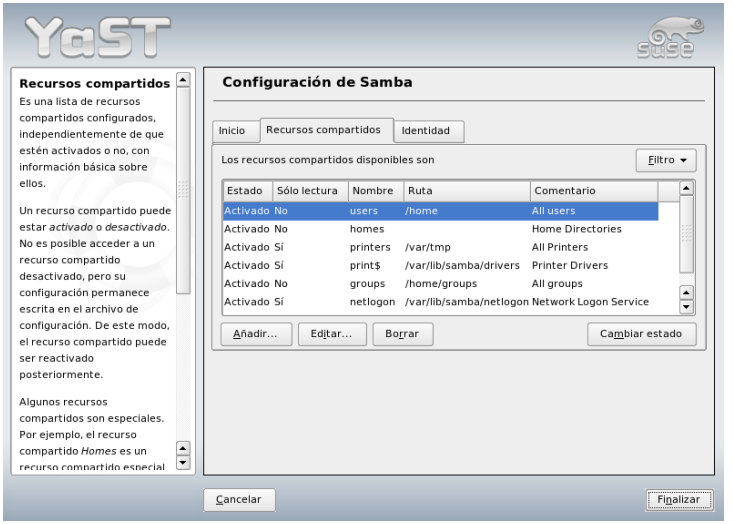

Figura 32.2: *Configuración de Samba: recursos compartidos*

recursos compartidos Samba deben estar activos. Para ello dispone del botón 'Cambiar estado' que, como su nombre indica, pasa del estado 'activado' a 'desactivado' y viceversa. Puede integrar nuevos recursos compartidos con el botón 'Añadir'.

En el menú 'Identidad' (figura **??** en esta página) puede especificar el dominio al que pertenece el ordenador ('Configuración básica') y decidir si debe emplearse un nombre de máquina alternativo ('Nombre NetBIOS') en la red.

32.4. Configuración de los clientes

Los clientes sólo pueden acceder al servidor Samba mediante TCP/IP. Actualmente no es posible utilizar NetBEUI o NetBIOS a través de IPX con Samba.

Figura 32.3: *Configuración de Samba: identidad*

32.4.1. Configuración de un cliente Samba con YaST

Puede configurar un cliente Samba para acceder fácilmente a recursos (archivos o impresora) en el servidor Samba. Para ello introduzca en el diálogo 'Grupo de trabajo SAMBA' el dominio o grupo de trabajo. El botón 'Examinar' muestra una lista de todos los grupos y dominios disponibles que pueden seleccionarse con el ratón. Al activar la opción 'Usar también la información SMB para la autentificación de Linux', la autentificación de usuarios se llevará a cabo también a través del servidor Samba. Una vez que ha definido todas las opciones, pulse 'Finalizar' para cerrar la configuración.

32.4.2. Windows 9x/ME

Windows 9x/ME ya incorpora el soporte de TCP/IP, pero al igual que en Windows for Workgroups no está incluido en la instalación estándar. Para instalar 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.

Sugerencia

Para usar una impresora conectada al servidor Samba, se recomienda instalar en el cliente el controlador general para impresoras PostScript o el utilizado para impresoras Postscript de Apple incluidos en la versión correspondiente de Windows. Después se conecta con la cola de impresión de Linux que acepta PostScript como formato de entrada.

Sugerencia

32.5. 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 la página del manual de `smb.conf` y en la de `socket(7)`. Puede obtener información adicional en el capítulo `Samba performance tuning` de `Samba-HOWTO-Collection`.

La configuración estándar en `/etc/samba/smb.conf` intenta proponer valores de amplio alcance orientándose a la configuración predeterminada 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.

Sugerencia

El equipo de Samba incluye en `Samba-HOWTO-Collection` una sección sobre la búsqueda de fallos. Asimismo, la sección V contiene instrucciones para comprobar paso a paso la configuración.

Sugerencia

El servidor proxy Squid

El caché proxy por excelencia para plataformas Linux/UNIX es Squid. En este capítulo se describe su configuración y los requisitos necesarios para su funcionamiento. También se explica cómo configurar un servidor proxy transparente, cómo obtener estadísticas sobre el uso del caché con la ayuda de programas como Calamaris y cachemgr o cómo filtrar contenidos web con la herramienta squidGuard.

33.1. ¿Qué es un caché proxy?

Squid se comporta como un caché proxy: recibe peticiones de objetos por parte de los clientes (en este caso navegadores web) y las reenvía al servidor. Cuando recibe los objetos solicitados del servidor, los envía al cliente y almacena una copia de los mismos en un caché de disco. La ventaja del caching consiste en que cuando varios clientes solicitan el mismo objeto, este puede proporcionárselo desde el caché de disco. De este modo, los clientes obtiene los datos mucho más rápidamente que si lo hicieran desde Internet y se reduce al mismo tiempo el volumen de transferencias en red.

Además del caching, Squid ofrece múltiples prestaciones tales como la definición de jerarquías de servidores proxy para distribuir la carga del sistema, establecer estrictas reglas de control de acceso para los clientes que quieran acceder al proxy, permitir o denegar el acceso a determinadas páginas web con ayuda de aplicaciones adicionales o producir estadísticas sobre las páginas web más visitadas y por tanto sobre los hábitos de navegación del usuario. 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.

33.2. Información general sobre cachés proxy

33.2.1. 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, haciendo que sea el proxy el que establezca todas las comunicaciones con la World Wide Web.

Si la configuración del cortafuegos incluye una zona desmilitarizada (DMZ), es allí donde se utilizará 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 la sección **??** en esta página se describe un método para configurar un proxy *transparente*.

33.2.2. 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, en el caso de una red local muy extensa conviene configurar un servidor proxy para cada subred y conectar estos a un proxy de jerarquía superior conectado a su vez 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 (Hypertext Transmission Protocol), 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. Estos 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.

Sugerencia

Para evitar duplicaciones de los objetos en varios cachés en la red se utilizan también 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.

Sugerencia

33.2.3. 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.

33.3. Requisitos 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 sobrestimar los requerimientos del sistema, ya que un Squid trabajando al límite de su capacidad puede repercutir negativamente en el funcionamiento de los servicios.

33.3.1. 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 milisegundos, que debe ser lo más bajo posible. Para lograr una velocidad elevada se recomienda utilizar discos duros rápidos. 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. Otra posibilidad para aumentar la velocidad consiste en el uso paralelo de varios discos duros o de Striping Raid Arrays.

33.3.2. 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 se dispone 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 memoria RAM para Squid.

33.3.3. Memoria RAM

La cantidad de memoria (RAM) 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 la sección **??** en esta página.

33.3.4. Potencia del procesador

Squid no es un programa que consuma mucha 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.

33.4. Arrancar Squid

Squid ya se encuentra preconfigurado en SUSE LINUX hasta el punto que se puede iniciar directamente después de la instalación. Para ello debe disponer de una red configurada de tal forma que sea posible acceder al menos a un servidor de nombres y a Internet, cuyos datos queremos guardar en el caché. Pueden aparecer problemas en caso de utilizar una conexión telefónica con configuración dinámica de DNS. En tales casos, 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`.

33.4.1. Comandos de inicio y parada

Para iniciar Squid, introduzca (como `root`) el comando `rcsquid start` en la línea de comando. 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/init.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 introduciendo los valores `localhost` como proxy y `3128` como puerto 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_acces deny all` a `http_acces 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 la sección **??** en esta página.

Cada vez que se produce un cambio en el archivo de configuración `/etc/squid/squid.conf`, Squid debe volver a cargarlo, lo que se realiza con el comando: `rcsquid reload`. De forma alternativa, también es posible reiniciar completamente Squid con `rcsquid restart`.

El comando `rcsquid status` determinar si el proxy se encuentra en ejecución y con `rcsquid stop` es posible detener 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, tras lo que todavía tiene que guardar los datos en el disco.

Aviso

Terminar Squid

Si Squid es terminado con un comando `kill` o bien `killall`, se pueden producir daños en el caché. Si la caché está dañado, ha de borrarse 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 `/var/squid/logs/cache.log` . 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 en el nivel de ejecución deseado. Vea la sección 2.7.7 en la página 78.

Al desinstalar Squid no se borrará ni la jerarquía caché ni los archivos de registro. Se deberá borrar manualmente el directorio `/var/cache/squid`.

33.4.2. Servidor DNS local

Se recomienda configurar un servidor DNS local incluso aunque el servidor proxy no controle su propio dominio. En ese caso actuará solamente como "DNS sólo caché" y de esta manera será capaz de resolver consultas DNS a través del servidor de nombres principal sin necesidad de realizar ninguna configuración especial (consulte a este respecto la sección **??** en esta página). La forma en la que esto se realiza depende de si se ha elegido DNS dinámico durante la configuración del acceso a Internet.

DNS dinámico Con el DNS dinámico, el servidor DNS es activado por el proveedor cuando se establece la conexión a Internet y el archivo local

`/etc/resolv.conf` se ajusta automáticamente. Esto sucede porque la variable sysconfig `MODIFY_RESOLV_CONF_DYNAMICALLY` tiene el valor `YES`. Asigne a esta variable el valor `NO` con el editor sysconfig de YaST (ver sección **??** en esta página). A continuación introduzca el servidor de nombres local en el archivo `/etc/resolv.conf` con la dirección IP `127.0.0.1` para `localhost`. De este modo, Squid siempre puede localizar el servidor de nombres local cuando se inicia.

Para poder acceder al servidor de nombres del proveedor, su nombre y dirección IP deben introducirse en el archivo de configuración `/etc/named.conf` en la sección `forwarders`. Como hemos visto arriba, el DNS dinámico realiza este proceso automáticamente cuando a la variable sysconfig `MODIFY_NAMED_CONF_DYNAMICALLY` se le asigna el valor `YES`.

DNS estático Con el DNS estático los ajustes no automáticos relativos a DNS se llevan a cabo cuando se establece la conexión. Así pues, no es necesario modificar las variables sysconfig pero sí introducir el servidor de nombres local en el archivo `/etc/resolv.conf` tal y como se ha descrito arriba. Asimismo, el servidor de nombres estático del proveedor y su dirección IP deben introducirse manualmente en el archivo `/etc/named.conf` en la sección `forwarders`.

Sugerencia

DNS y el cortafuegos

Si ha activado un cortafuegos en el sistema, asegúrese de que las consultas DNS puedan atravesarlo.

Sugerencia

33.5. El archivo de configuración /etc/squid/squid.conf

La configuración de Squid se almacena en el archivo de configuración `/etc/squid/squid.conf`. 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 recomendable 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.

Sugerencia

Adaptar el archivo de configuración tras una actualización

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 `squid.conf`, es posible que no funcione correctamente debido a modificaciones en algunas opciones o a los nuevos cambios en la nueva versión.

Sugerencia

33.5.1. Opciones generales de configuración (selección)

http_port 3128 Este es el puerto en el que Squid atenderá las peticiones de los clientes. El puerto por defecto es `3128`, aunque también suele emplearse `8080`. Es posible especificar varios puertos separándolos por espacios en blanco.

cache_peer ⟨***hostname***⟩ ⟨***type***⟩ ⟨***proxy-port***⟩ ⟨***icp-port***⟩
Esta opción permite especificar otro servidor proxy como "padre" (parent), por ejemplo si quiere usar el de su proveedor. En la opción ⟨*hostname*⟩ se especifica el nombre y la dirección IP del proxy al que nos vayamos a conectar, en la opción ⟨*type*⟩, especificamos `parent`. Para ⟨*proxy-port*⟩, se debe escribir el número de puerto especificado por el operador del "padre" para los navegadores (normalmente se utiliza el `8080`). Como ⟨*icp-port*⟩ puede introducirse `7` o bien `0` si no se conoce el puerto ICP del proxy padre y su uso carece de interés para el proveedor. Asimismo, `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 de registro.

cache_log /var/log/squid/cache.log ruta para archivos de registro.

cache_store_log /var/log/squid/store.log
Ruta para archivos de registro.

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 se le asigna a la entrada el valor *on*, será posible obtener archivos de registro en formato legible. Sin embargo, algunos programas de evaluación no pueden interpretarlos.

client_netmask 255.255.255.255 Esta entrada permite enmascarar las direcciones IP en los archivos de registro para ocultar la identidad de los clientes. Especificando en esta opción el valor `255.255.255.0`, la última cifra de la dirección IP se interpretará como cero.

ftp_user Squid@ Esta opción se utiliza para definir la contraseña usada por Squid para realizar el registro (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 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 el comando `squid -k rotate`. Los archivos serán enumerados durante este proceso y, una vez alcanzado el valor especificado, el archivo más antiguo será sobreescrito. El valor que se utiliza normalmente es `0`, ya que para archivar y borrar archivos de registro en SUSE LINUX se usa un cronjob que se encuentra en el archivo de configuración `/etc/logrotate/squid`.

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 desactivar esta opción con el valor *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. No obstante, si se dispone de una conexión telefónica, a veces puede ocurrir que no sea posible acceder a Internet. Si esto sucede, 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. Este debe estar ya introducido en la opción *cache_peer*. Si como ⟨*acl_name*⟩ se especifica 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.

33.5.2. Listas de control de acceso o ACLs

Squid dispone de un elaborado sistema para controlar el acceso al proxy que, gracias al uso de ACLs, puede ser configurado de forma fácil y flexible. Se trata de listas de normas procesadas secuencialmente. Las ACLs deben ser definidas antes de poder utilizarse. Algunas ACLs como *all* y *localhost* ya están predefinidas. La mera definición de una ACL no tiene ningún efecto. Es necesario que se aplique por ejemplo en combinación 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. 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 que contenga, por ejemplo, nombres de máquinas, direcciones IP o bien URLs. A continuación algunos ejemplos:

```
acl usuarios srcdomain .mi-dominio.com
acl profesores src 192.168.1.0/255.255.255.0
acl alumnos src 192.168.7.0-192.168.9.0/255.255.255.0
acl mediodía time MTWHF 12:00-15:00
```

http_access allow <acl_nombre> *http_access* determina a quién le está permitido usar el proxy y quién puede acceder a Internet. Para ello deben definirse ACLs que permitan o denieguen el acceso mediante *allow* o *deny* (*localhost* y *all* ya han sido definidas con anterioridad). Se puede crear una lista completa de entradas *http_access* que será procesada de arriba a abajo y, dependiendo de qué regla pueda aplicarse en primer lugar, se permitirá o no el acceso a Internet para cada URL. Por eso la última entrada de todas debe ser *http_access deny all*. En el ejemplo siguiente *localhost* (el ordenador local) 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
```

Para mantener el orden se recomienda insertar la lista con las entradas *http_access* propias en el archivo `/etc/squid/squid.conf` entre las líneas

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
# CLIENTS
```

y

```
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 URLs no deseadas. El acceso a Internet puede ser controlado individualmente para varios grupos de usuarios con la ayuda de la autentificación por proxy y listas de control de acceso apropiadas. squidGuard es un paquete independiente que se debe instalar y configurar separadamente.

auth_param basic program /usr/sbin/pam_auth
Si los usuarios deben ser autentificados en el proxy, se puede especificar un programa como pam_auth que realice esta función. Cuando se accede a pam_auth por primera vez, el usuario verá una pantalla de login donde deberá introducir el nombre de usuario y la contraseña. Además será necesario especificar una ACL 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* puede también sustituirse por una lista de usuarios permitidos o por la ruta a esa 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*>, la regla será válida para todos los clientes. Para ello deberá ejecutar un daemon denominado

ident en todos los clientes. En Linux, se puede utilizar para este propósito el paquete pidentd; en el caso de `Windows`, hay software libre disponible que se puede descargar de Internet. Para asegurar que sólo se permita el acceso a clientes correctamente identificados, se deberá igualmente especificar otra ACL tal y como se define a continuación:

```
acl identhosts ident REQUIRED

http_access allow identhosts
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 autentificación se repite para cada petición.

33.6. 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 este 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 clientes utilicen un proxy para navegar por Internet.
- Es necesario que todos los clientes utilicen un proxy, sean los usuarios conscientes de ello o no.
- El proxy de una red cambia de ubicación pero 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.

33.6.1. Configuración del kernel

Primero hay que comprobar si el kernel del servidor proxy dispone de soporte para proxy transparente. El kernel incluido en SUSE LINUX ya está configurado en consecuencia. Si no lo soporta, habrá que añadir estas opciones al kernel y compilarlo de nuevo. Puede obtener más información sobre este proceso en el capítulo **??** en esta página.

33.6.2. Opciones de configuración en /etc/squid/squid.conf

Para implementar un proxy transparente es necesario activar las siguientes opciones del archivo `/etc/squid/squid.conf`:

- `httpd_accel_host` virtual
- `httpd_accel_port` El número de puerto donde se encuentra el servidor HTTP.
- `httpd_accel_with_proxy` on
- `httpd_accel_uses_host_header` on

33.6.3. Configuración del cortafuegos con SuSEfirewall2

Todas las peticiones que se reciban a través del cortafuegos deben ser redirigidas al puerto de Squid por medio de una norma de reenvío de puertos. Para la configuración utilizaremos la herramienta SuSEfirewall2 incluida en la distribución. El archivo de configuración correspondiente se encuentra en `/etc/sysconfig/SuSEfirewall2`. Este archivo está formado por diferentes entradas muy bien documentadas. Aunque sólo se quiera implementar un proxy transparente, es necesario configurar algunas opciones del cortafuegos:

- Dispositivo apuntando a Internet: `FW_DEV_EXT`="eth1"
- Dispositivo apuntando a la red: `FW_DEV_INT`="eth0"

Aquí pueden definirse puertos y servicios (ver `/etc/services`) del cortafuegos a los que se podrá acceder desde redes no seguras como Internet. En este ejemplo sólo se especifican servicios web hacia el exterior:

```
FW_SERVICES_EXT_TCP="www"
```

Aquí pueden definirse puertos y servicios (ver `/etc/services`) del cortafuegos a los que se podrá acceder desde la red segura (interna) a través de TCP y UDP:

```
FW_SERVICES_INT_TCP="domain www 3128"
FW_SERVICES_INT_UDP="domain"
```

Accedemos a servicios web y al programa Squid (cuyo puerto predeterminado es `3128`). El servicio "domain" especificado anteriormente se trata del DNS o Domain Name Service. Lo más normal es utilizar este servicio, pero en caso contrario, se elimina de las entradas superiores y se asigna a la opción siguiente el valor `no`:

```
FW_SERVICE_DNS="yes"
```

La opción más importante es la número `15`:

Ejemplo 33.1: *Opción 15 de la configuración del cortafuegos*

```
#
# 15.)
# Which accesses to services should be redirected to a local port
# on the firewall machine?
#
# This can be used to force all internal users to surf via your
# Squid proxy, or transparently redirect incoming web traffic to
# a secure web server.
#
# Choice: leave empty or use the following explained syntax of
# redirecting rules, separated with spaces.
# A redirecting rule consists of 1) source IP/net,
# 2) destination IP/net, 3) original destination port and
# 4) local port to redirect the traffic to, separated by a colon,
# e.g. "10.0.0.0/8,0/0,80,3128 0/0,172.20.1.1,80,8080"
#
```

Los comentarios 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`. Este valor es un comodín que significa "a cualquier dirección". A continuación, el número de puerto original al que fueron dirigidas las peticiones y, finalmente, el puerto a donde redirigimos las peticiones. Como Squid soporta 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 `START_FW`:

Inicie Squid tal y como se describe en la sección **??** en esta página. 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 -O dirección_IP`.

33.7. 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.

33.7.1. 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
```

Apache se está ejecutando en el ordenador. Si no es así, ejecute el comando `rcapache start` para iniciar Apache con la configuración predeterminada de SUSE LINUX. El último paso es copiar el archivo `cachemgr.cgi` al directorio de Apache `cgi-bin`:

```
cp /usr/share/doc/packages/squid/scripts/cachemgr.cgi /srv/www/cgi-bin/
```

33.7.2. ACLs para el administrador de caché en /etc/squid/squid.conf

Hay algunas opciones configuradas ya por defecto en el archivo de configuración para el administrador de caché: la primera ACL es la más importante, ya que el administrador de caché tratará de comunicarse con Squid mediante el protocolo cache_object.

```
acl manager proto cache_object

acl localhost src 127.0.0.1/255.255.255.255
```

Las siguientes normas de acceso también deben estar incluidas:

```
http_access allow manager localhost

http_access deny manager
```

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 el ejemplo **??** en esta página.

Ejemplo 33.2: *Reglas de acceso*

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl webserver src 192.168.1.7/255.255.255.255 # webserver IP
```

También son necesarias las reglas siguientes del ejemplo **??** en esta página.

Ejemplo 33.3: *Reglas de acceso*

```
http_access allow manager localhost

http_access allow manager webserver
http_access deny manager
```

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`.

33.7.3. Leer las estadísticas

En primer lugar, diríjase a la página web correspondiente: `http://webserver.example.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 `http://www.squid-cache.org/Doc/FAQ/FAQ-9.html`.

33.8. 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.

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.

Instale el paquete `squidGuard`. 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 consiste crear una página web que será la página que mostrará el mensaje de "acceso denegado" o una página CGI más o menos compleja 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 configurar Squid de forma 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 distintos procesos de redireccionamiento o "redirect" (en este caso procesos de squidGuard) que se ejecutan en la máquina. squidGuard es suficientemente rápido para procesar grandes cantidades de solicitudes: 100.000 consultas en 10 segundos en un Pentium 500 MHz 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 en Squid con `rcsquid reload`. A continuación ya se puede comprobar la configuración con cualquier navegador.

33.9. 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 estos estén cronológicamente ordenados, es decir, primero los archivos más antiguos. Las diferentes opciones:

-a muestra 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 es:

```
cat access.log.2 access.log.1 access.log | calamaris -a -w \
> /usr/local/httpd/htdocs/Squid/squidreport.html
```

Este comando guarda el informe en el directorio del servidor web. Se necesita Apache para poder visualizarlo.

Otro completo generador de informes es SARG (Squid Analysis Report Generator). Puede obtener información adicional sobre SARG en: `http://web.onda.com.br/orso/`

33.10. Información adicional sobre Squid

Visite la página web de Squid: `http://www.squid-cache.org/`. Aquí encontrará la "Squid User Guide" junto con una extensa colección de FAQs sobre Squid.

Después de la instalación, el Mini-Howto sobre proxys transparentes del paquete `howtoenh` está disponible en `/usr/share/doc/howto/en/txt/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/`

Parte IV

Administración

Seguridad en Linux

El enmascaramiento (masquerading) y el cortafuegos (firewall) se ocupan de controlar el tráfico e intercambio de datos. La SSH (Secure Shell) permite al usuario realizar una conexión codificada con un ordenador remoto. La codificación de archivos o particiones enteras protegen sus datos en caso de que terceras personas accedan al sistema. Además de instrucciones de carácter puramente técnico, al final del capítulo encontrará un apartado general sobre aspectos de seguridad en redes Linux.

34.1. Cortafuegos y enmascaramiento

El kernel de Linux dispone de funciones para administrar paquetes de red que se utilizan, por ejemplo, cuando Linux se emplea en un entorno de red donde debe separar diversos sectores externos e internos. La infraestructura de Netfilter ofrece todas las herramientas necesarias para utilizar un sistema Linux como un cortafuegos eficaz entre distintas redes. iptables, una estructura genérica de tablas con reglas de filtrado, permite el control preciso sobre los paquetes de datos que deben y no deben atravesar el cortafuegos. SuSEfirewall2 y el módulo correspondiente de YaST facilitan la configuración de un filtro de paquetes.

34.1.1. Filtrado de paquetes con iptables

Netfilter e iptables se encargan de filtrar, modificar y traducir por medio de NAT (*Network Address Translation*) paquetes de la red. Los criterios de filtrado y las acciones asociadas se guardan en secuencias o cadenas que se aplican de forma sucesiva cuando se recibe un paquete de red. El comando `iptables` sirve para editar las reglas que se encuentran en tablas.

En Linux existen tres tablas para las diferentes funciones de un filtro de paquetes:

filter En esta tabla, que contiene la mayoría de reglas, se realiza el verdadero filtrado de paquetes y se definen también las reglas para aceptar (`ACCEPT`) o rechazar (`DROP`) paquetes.

nat Esta parte define la modificación de las direcciones de origen y destino de los paquetes. El enmascaramiento o *masquerading*, que se utiliza para conectar una pequeña red privada a Internet, es un caso especial de NAT.

mangle Las reglas en este apartado permiten editar valores en el encabezamiento del paquete IP (por ejemplo el *Type of Service*).

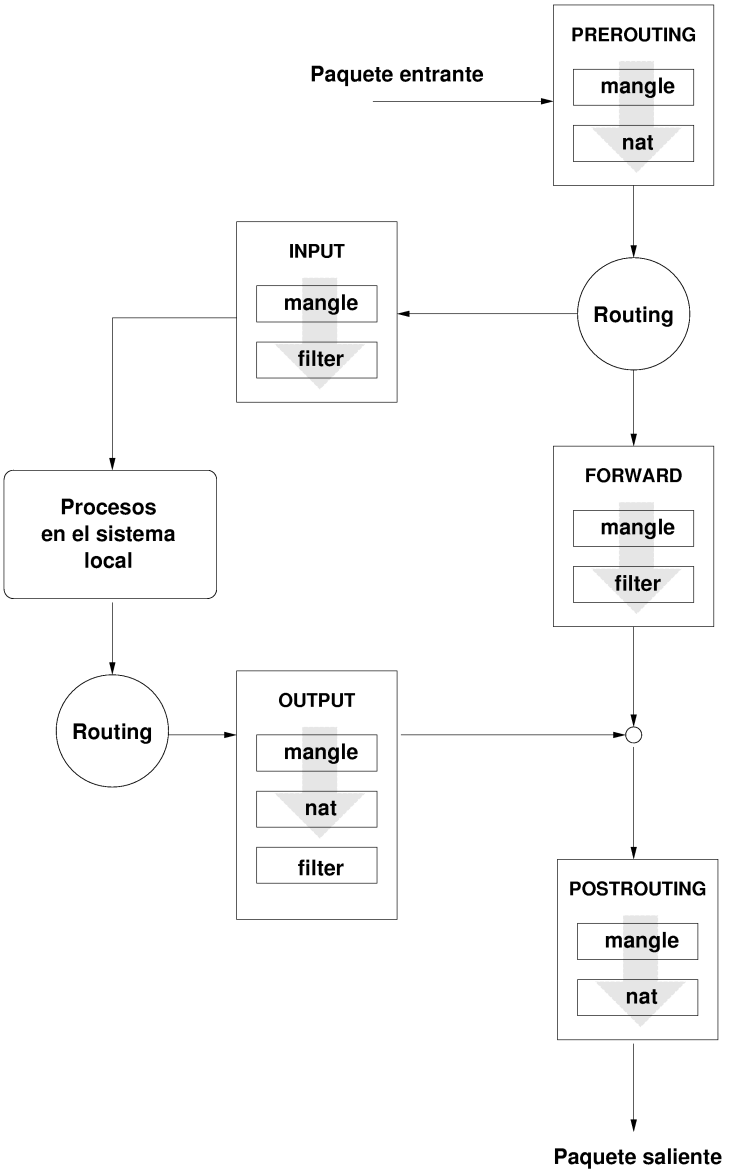

Figura 34.1: *iptables: rutas de un paquete por el sistema*

Dentro de las tablas mencionadas existen varias cadenas predefinidas por las que tienen que pasar los paquetes:

PREROUTING Esta cadena se aplica a paquetes que acaban de llegar al sistema.

INPUT Esta cadena se aplica a paquetes que se ocupan de procesos internos del sistema.

FORWARD Esta cadena se aplica a paquetes que atraviesan el sistema sin ser modificados.

OUTPUT Esta cadena se aplica a paquetes generados en el propio sistema.

POSTROUTING Esta cadena es para todos los paquetes que salen del sistema.

La figura **??** en esta página muestra la ruta de un paquete de red al pasar por el sistema. Para una mayor claridad, las tablas están agrupadas por cadenas aunque en realidad las cadenas se organizan dentro de las tablas.

En el caso más sencillo un paquete destinado al propio sistema aparece en la interfaz `eth0` y pasa primero a la cadena `PREROUTING` de la tabla `mangle`. Posteriormente pasa a la cadena `PREROUTING` de la tabla `nat`. En el siguiente paso de enrutado se averigua que el paquete está destinado a un proceso del sistema propio. Tras pasar las cadenas `INPUT` dentro de las dos tablas `mangle` y `filter` el paquete llega a su destino, salvo que las reglas de la tabla `filter` lo impidan.

34.1.2. Fundamentos del enmascaramiento

El enmascaramiento es un caso especial de NAT (Network Address Translation), la traducción de direcciones de red. Se utiliza para conectar una pequeña LAN con direcciones IP privadas (ver sección **??** en esta página) a Internet con sus direcciones públicas. Las direcciones privadas de los ordenadores dentro de la LAN se traducen en direcciones públicas para el acceso a Internet. El enrutador, que se encarga del enlace entre LAN e Internet, realiza este proceso. El principio en el que se sustenta es bastante sencillo: 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). Una de estas interfaces conecta su sistema con el exterior mientras que otra o varias conectan el ordenador con los otros ordenadores de la red. En este caso existen en la red local varios ordenadores conectados a la tarjeta de red del enrutador Linux (en este ejemplo `eth0`). Los ordenadores de la red envían todos los paquetes que no están dirigidos a la red propia al enrutador predeterminado o bien a la pasarela predeterminada.

Importante

Máscaras de red uniformes

Al configurar la red, asegúrese de que las direcciones de difusión (broadcast) y las máscaras de red coinciden. De lo contrario, la red no funciona correctamente ya que los paquetes de red no pueden ser enrutados.

Importante

Cuando uno de los ordenadores de la red envía un paquete a Internet, éste llega al enrutador predeterminado. El enrutador debe estar configurado de tal forma que reenvíe dichos paquetes. Por razones de seguridad, la configuración predeterminada de SUSE LINUX no lo hace. Modifique la variable `IP_FORWARD` en el archivo `/etc/sysconfig/sysctl` y asígnele el valor `IP_FORWARD=yes`.

La máquina destino sólo conoce el enrutador y no el ordenador concreto de la red interna desde el que se envió el paquete, ya que este queda escondido detrás del enrutador. De ahí viene el concepto enmascarar (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 llegue al ordenador correcto de la red local.

Puesto que la ruta de los paquetes desde el exterior al interior depende de la tabla de enmascaramiento, no hay ninguna posibilidad de establecer una conexión hacia dentro. No existiría ninguna entrada en la tabla para tal conexión. A toda conexión establecida se le ha asignado además un estado en la tabla, de forma que esa entrada de la tabla no pueda ser utilizada por una segunda conexión.

Como consecuencia se producen problemas con algunas aplicaciones, como por ejemplo con ICQ, cucme, IRC (DCC, CTCP) y FTP (en modo PORT). Netscape, el programa estándar de FTP y muchas otras utilizan el modo PASSV, que causa pocos problemas con el filtrado de paquetes y el enmascaramiento.

34.1.3. Fundamentos del cortafuegos

El cortafuegos (firewall) es de hecho el término más extendido para un mecanismo que conecta dos redes y que pretende controlar el tráfico de datos en la medida de lo posible. El tipo de cortafuegos que presentamos aquí se debería llamar con más precisión *filtro de paquetes*. Un filtro de paquetes regula el paso de los mismos en función de criterios como el protocolo, el puerto y la dirección IP. De

esta forma, también puede interceptar paquetes que, debido a su direccionamiento, no deberían entrar en la red. Si por ejemplo desea permitir el acceso a su servidor web, debe desbloquear el puerto correspondiente. Si la dirección de estos paquetes es correcta (por ejemplo el servidor web como destino), no se examinará su contenido. Por lo tanto, 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 estructura como por ejemplo un filtro de paquetes al que se le añaden otras aplicaciones de pasarela/proxy. El filtro rechazaría paquetes que se dirigiesen, por ejemplo, a puertos que no estuvieran desbloqueados y sólo dejarían pasar paquetes para una aplicación de pasarela. Este proxy actúa como interlocutor en la comunicación con el servidor que quiere establece una conexión con nosotros. En este sentido se puede considerar a un proxy de este tipo como una máquina de enmascaramiento a 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 forma que las solicitudes de páginas html pasen primero por la memoria del proxy y, sólo en caso de no encontrar allí la página, sean enviadas por el proxy a Internet. El proxy-suite de SUSE contiene un servidor proxy para el protocolo FTP.

A continuación nos centraremos en el filtro de paquetes de SUSE LINUX. Puede obtener información adicional y enlaces sobre el cortafuegos en el COMO incluido en `howto`. Si el paquete `howto` está instalado, también lo puede leer con el comando `less /usr/share/doc/howto/en/txt/Firewall-HOWTO.gz`

34.1.4. SuSEfirewall2

SuSEfirewall2 es un script que convierte las variables definidas en `/etc/sysconfig/SuSEfirewall2` en un conjunto de reglas iptables. SuSEfirewall2 conoce tres zonas de seguridad (de las que sólo las dos primeras se tienen en cuenta en el siguiente ejemplo de configuración):

Zona externa El ordenador debe estar protegido de la red externa porque no existe ningún control sobre esta red. Habitualmente la red externa es Internet, pero también se puede tratar de otra red desprotegida (por ejemplo una WLAN).

Zona interna Esta es la LAN propia. Si las direcciones IP dentro de la LAN son de la zona privada (ver sección ?? en esta página), es necesario utilizar NAT (Network Address Translation) para que la red interna pueda acceder a la externa.

Zona desmilitarizada (DMZ) Se puede acceder a los ordenadores de esta zona desde la red externa e interna, pero no tienen acceso a la red interna. Esta configuración protege además la red interna de la externa, ya que los ordenadores de la DMZ no pueden acceder a ordenadores internos.

iptables suprime cualquier tráfico de red que no sea explícitamente autorizado por las reglas. Por eso toda interfaz que envíe paquetes a una red debe estar asignada a una de las zonas y es necesario definir los servicios o protocolos permitidos para cada una de la zonas. No obstante, las reglas se aplican exclusivamente a paquetes de origen remoto; los paquetes de origen local se envían siempre.

La configuración puede realizarse con YaST (ver sección Configuración con YaST en esta página) o bien editando directamente el archivo `/etc/sysconfig/SuSEfirewall2` que contiene comentarios detallados en inglés. Además puede encontrar algunos escenarios de aplicación en `/usr/share/doc/packages/SuSEfirewall2/EXAMPLES`.

Configuración con YaST

Importante

Configuración automática del cortafuegos

Después de la instalación, YaST se encarga de iniciar automáticamente un cortafuegos en todas las interfaces configuradas por el usuario. YaST utiliza además las opciones 'Abrir cortafuegos para la interfaz seleccionada' o 'Puerto abierto en el cortafuegos' incluidas en los módulos de configuración de servidor, para adaptar la configuración generada automáticamente tan pronto como un servicio es configurado y activado en el sistema. El diálogo del módulo de servidor puede contener también un botón de 'Detalles' que le permite activar servicios y puertos adicionales. El módulo de YaST para configurar el cortafuegos puede utilizarse para activar o desactivar el cortafuegos o para modificar su configuración de forma independiente.

Importante

La configuración gráfica con YaST se realiza en el Centro de Control de YaST. Una vez allí, seleccione el apartado 'Cortafuegos' del menú 'Seguridad y usuarios'. La configuración está dividida en siete secciones a las que puede acceder directamente a través de la estructura de árbol en la parte izquierda de la pantalla:

Inicio Aquí puede definir el comportamiento de inicio. En una instalación estándar, SuSEfirewall2 ya se ejecuta en el sistema recién instalado. En esta sección también es posible iniciar y detener el cortafuego. El botón 'Guardar la configuración y reiniciar cortafuegos' le permite probar la configuración actual del cortafuegos.

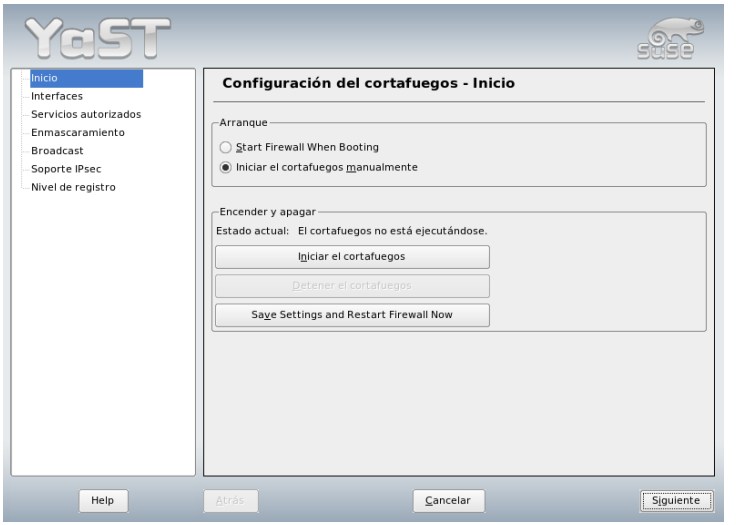

Figura 34.2: *Configuración del cortafuegos en YaST*

Interfaces Este diálogo contiene una lista de todas las interfaces de red. Para eliminar una interfaz de una zona, selecciónela en la lista, pulse 'Cambiar' y escoja 'Sin zona asignada'. Si desea añadir una interfaz a una zona, selecciónela, pulse 'Cambiar' y escoja una de las zonas disponibles. Con el botón 'Personalizar' puede crear una interfaz de configuración personalizada.

Servicios autorizados Esta opción le permite ofrecer desde el sistema servicios a una zona protegida. Por defecto, sólo la zona externa está protegida. En este caso es necesario autorizar explícitamente los servicios que han de ser accesibles para equipos externos. Para ello, active el servicio correspondiente después de haber seleccionado la zona en 'Servicios autorizados para zona seleccionada'.

Enmascaramiento El enmascaramiento le permite ocultar la red interna de redes

externas como Internet, y además posibilita el acceso de la red interna a la red externa de forma transparente. Las peticiones de la red externa a la interna se bloquean, mientras que de cara al exterior, las peticiones de la red interna parecen tener su origen en el servidor de enmascaramiento.

Si determinados servicios de una máquina interna deben estar disponibles para la red externa, puede añadir reglas especiales de redireccionamiento para el servicio correspondiente.

Broadcast En este diálogo se configuran los puertos UDP que permiten las llamadas de difusión general o broadcast. Introduzca separados por espacios los números de puerto o servicios que deben añadirse a una zona. Vea también el archivo `/etc/services`.

Aquí también puede activar que se lleve protocolo de los broadcasts que han sido rechazados. No obstante, esto puede resultar problemático porque los sistemas Windows utilizan el broadcast para saber unos de otros, generando muchos paquetes no autorizados.

Soporte IPsec Este diálogo le permite configurar si el servicio IPsec debe permitirse desde la red externa. En la sección 'Detalles' puede definir qué paquetes son de confianza.

Nivel de registro Existen dos reglas principales para el registro: paquetes autorizados o no autorizados. Los autorizados son aceptados (ACCEPTED), mientras que los no autorizados son desechados (DROPPED) o rechazados (REJECTED). Para ambos tipos de paquetes puede seleccionar 'Registrar todos', 'Registrar sólo críticos' o 'No registrar ninguno'.

Una vez completada la configuración del cortafuegos, salga del diálogo con 'Siguiente'. A continuación aparece un resumen de la configuración del cortafuegos en función de las zonas donde puede revisar las opciones de configuración seleccionadas. El resumen incluye todos los servicios, puertos y protocolos que han sido autorizados. Pulse 'Atrás' para volver a la configuración o bien 'Aceptar' para guardarla.

Configuración manual

A continuación se muestra paso a paso cómo se realiza una configuración adecuada. En cada punto se indica si es válido para el enmascaramiento o para el cortafuegos. En los archivos de configuración también se menciona una DMZ (zona desmilitarizada) que no se tratará con más detalle en estas líneas, ya que se

utiliza exclusivamente en redes complejas de grandes organizaciones (empresas, etc.) y su configuración presenta un alto grado de dificultad.

Active en primer lugar SuSEfirewall2 con el módulo Servicios del sistema (niveles de ejecución) de YaST para que se ejecute en el nivel actual (probablemente 3 ó 5). De este modo, se introducirán enlaces simbólicos para los scripts SuSEfirewall2_* en los directorios `/etc/init.d/rc?.d/`.

`FW_DEV_EXT` (cortafuegos, enmascaramiento)
La interfaz que apunta hacia Internet. En caso de módem, emplee `ppp0`, para RDSI `ippp0` y `dsl0` para las conexiones DLS. La interfaz para la ruta predeterminada utiliza `auto`.

`FW_DEV_INT` (cortafuegos, enmascaramiento)
Indique aquí la interfaz que apunta a la red interna o "privada" (por ejemplo `eth0`). Si no hay red interna se deja vacío.

`FW_ROUTE` (cortafuegos, enmascaramiento)
Si necesita enmascaramiento, introduzca aquí `yes`. Los ordenadores internos no son visibles desde fuera porque tienen direcciones IP privadas (por ejemplo `192.168.x.x`) cuyos paquetes no son enrutados en Internet.

Con un cortafuegos sin enmascaramiento, escoja aquí `yes` para 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 a las máquinas internas desde fuera.

`FW_MASQUERADE` (enmascaramiento) Si necesita enmascaramiento, introduzca `yes`. Con ello, las máquinas internas obtienen una conexión a Internet prácticamente directa. Tenga en cuenta que el acceso de la red interna a Internet a través de un servidor proxy es más seguro. El enmascaramiento no es necesario para los servicios que proporciona un servidor proxy.

`FW_MASQ_NETS` (enmascaramiento) Indique aquí el ordenador o red para la que se realizará enmascaramiento. 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_INT` (cortafuegos)
Introduzca `yes` si desea proteger también el ordenador que actúa como cortafuegos. Para ello debe desbloquear explícitamente los servicios disponibles para la red interna. Vea también `FW_SERVICES_INT_TCP` y `FW_SERVICES_INT_UDP`.

FW_SERVICES_EXT_TCP (cortafuegos)
Introduzca aquí los servicios a los que se debe tener acceso. Para un ordenador particular que no ofrece ningún servicio no escriba nada.

FW_SERVICES_EXT_UDP (cortafuegos)
Déjelo vacía a menos que utilice un servidor UDP al que se deba poder acceder desde el exterior. Entre los servicios que utilizan UDP se encuentran servidores DNS, IPSec, TFTP y DHCP, entre otros. En ese caso, indique aquí los puertos UDP adecuados.

FW_SERVICES_INT_TCP (cortafuegos)
Aquí se definen los servicios disponibles para la red interna. Las entradas son similares a las de `FW_SERVICES_EXT_TCP`, pero aquí se refieren a la red *interna*. Sólo es necesario configurar esta variable si `FW_PROTECT_FROM_INT` ha sido activado.

FW_SERVICES_INT_UDP (cortafuegos)
Ver FW_SERVICES_INT_TCP.

FW_STOP_KEEP_ROUTING_STATE (cortafuegos)
Si el acceso a Internet se realiza a través de diald o RDSI (llamada bajo demanda), introduzca `yes`.

Con este paso se completa la configuración. Ahora sólo queda probar el cortafuegos. Para crear las reglas de filtrado, ejecute como usuario `root` el comando `SuSEfirewall2 start`. A efectos de prueba, puede ejecutar por ejemplo un `telnet` desde fuera para ver si la conexión realmente se rechaza. A continuación, consulte las entradas en `/var/log/messages`. Su aspecto debería ser similar al siguiente:

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

Existen otros paquetes para probar la configuración del cortafuegos, como por ejemplo nmap o nessus. Después de instalar los paquetes respectivos, la documentación de nmap se encuentra en `/usr/share/doc/packages/nmap` y la de nessus en el directorio `/usr/share/doc/packages/nessus-core`.

34.1.5. Información adicional

En el directorio `/usr/share/doc/packages/SuSEfirewall2` se encuentra la documentación actualizada del paquete `SuSEfirewall2`. La página web del proyecto netfilter/iptables, `http://www.netfilter.org`, proporciona abundante documentación en varios idiomas.

34.2. SSH: trabajar de forma segura en red

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 sin la clave 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.

34.2.1. 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. En la configuración estándar, el acceso a un sistema SUSE LINUX únicamente es posible con las herramientas OpenSSH y sólo en el caso de que el cortafuegos permita el acceso.

34.2.2. 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. Después de introducir el comando, se nos preguntará la contraseña en el sistema sol.

Después de haber conseguido una autenticación válida se podrá trabajar tanto desde la línea de comandos, por ejemplo con el comando `ls`, como de forma interactiva, por ejemplo con YaST. Si quiere diferenciar el nombre de usuario local del usuario en el sistema remoto, hágalo por ejemplo con `ssh -l juan sol` o bien con `ssh juan@sol`.

Además, ssh nos ofrece la posibilidad ya conocida en rsh de ejecutar comandos en un sistema remoto. 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 sol "uptime; mkdir tmp"
tux@sol'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.

34.2.3. Copia segura: scp

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 (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, en el directorio `backup/` en el ordenador sol.

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.

34.2.4. Transmisión segura de archivos: sftp

Otra posibilidad para la transferencia segura de archivos 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.

34.2.5. El daemon SSH (sshd) del lado del servidor

Para que se puedan utilizar los programas cliente ssh y scp, en segundo plano se debe ejecutar un servidor, 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 por ejemplo 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 (encrypt) una clave que varía de sesión en sesión (session key) y que se envía al servidor SSH. Además indica al servidor el tipo de cifrado (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.nroff`). 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 este en el archivo `~/.ssh/known_hosts`.

34.2.6. Mecanismos de autenticación de SSH

Ahora 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.

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; estos podrían ser, por ejemplo, los archivos `id_rsa` y `id_rsa.pub`.

El comando `ssh-keygen -p -t rsa` o `ssh-keygen -p -t dsa` sirve para cambiar la contraseña antigua. 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 por ejemplo 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 (por ejemplo 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`.

34.2.7. X, autenticación 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` traspasa 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 siguiente comando reenvía todas las consultas hechas al puerto 110 (POP3) en tierra al puerto POP3 de sol:

```
ssh -L 110:sol:110 tierra
```

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`. 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`.

34.3. Codificación de archivos y particiones

34.3.1. Escenarios de aplicación

Cualquier usuario posee datos confidenciales que no deben mostrarse a terceras partes no autorizadas. Cuanto más se trabaje de forma móvil o en red, más en serio debe tomarse el tema de la seguridad en relación con los datos. Se recomienda codificar archivos o particiones enteras cuando terceras partes tengan acceso al sistema, bien sea físicamente o a través de una conexión de red. La siguiente lista menciona algunos escenarios de aplicación posibles:

Ordenadores portátiles Si normalmente trabaja de forma móvil y suele transportar datos confidenciales en el portátil, se recomienda codificar las particiones correspondientes en el disco duro. En caso de pérdida o robo del portátil, los datos que se hayan guardado en una partición codificada o en un sistema de archivos codificado basado en un archivo estarán a salvo de miradas indiscretas.

Medios extraíbles El riesgo de robo en el caso de los sticks USB o discos duros externos es el mismo que en el caso de un portátil. Un sistema de archivos codificado le ofrece también aquí protección de cara a terceros.

34.3.2. Configuración con YaST

YaST le ofrece la posibilidad de codificar archivos o directorios tanto durante la instalación como en el sistema instalado. Un sistema de archivos codificado puede crearse siempre, ya que se integra perfectamente en la estructura existente de particiones. Por su parte, una partición codificada sólo puede crearse cuando la estructura de particiones proporcione a tal efecto una partición dedicada. El particionamiento estándar sugerido por YaST durante la instalación no prevé espacio adicional para una partición codificada. Por lo tanto, en este caso ha de modificar manualmente la estructura de particionamiento para poder crear una partición codificada.

Configuración de una partición codificada durante la instalación

Aviso

Contraseña

Tenga en cuenta las advertencias de seguridad a la hora de definir la contraseña y recuerde bien ésta. En caso de olvidar la contraseña, no podrá volver a acceder a los datos codificados.

Aviso

En el diálogo avanzado de particionamiento ('Particionamiento en modo experto') descrito en la sección 2.7.5 en la página 73, seleccione el botón 'Crear' para crear una partición codificada como si se tratara de una partición cualquiera. A continuación se abre un diálogo donde puede introducir los parámetros de particionamiento. Introduzca aquí el tipo de formato y el punto de montaje de la nueva partición y pulse 'Sistema de archivos codificado'. En el siguiente diálogo puede introducir la contraseña que va a utilizar, la cual debe escribirse dos veces por razones de seguridad. La partición codificada se crea al abandonar el diálogo de particionamiento con 'OK'. La próxima vez que inicie el sistema deberá introducir la contraseña para que la partición codificada pueda montarse.

Si no desea montar la partición codificada durante el arranque, deje vacío el apartado correspondiente a la contraseña y responda negativamente a la pregunta sobre la repetición de la contraseña. En este caso, el sistema de archivos codificado no se montará y el resto del sistema será iniciado como de costumbre. El montaje automático de una partición codificada durante el arranque debilita el concepto de seguridad subyacente. Esto se debe a que la partición está disponible para todos los usuarios una vez que el sistema ha arrancado, a no ser que vuelva a desmontarse inmediatamente después de acceder a ella. Por lo tanto, esta opción sólo tiene sentido si desea proteger contra robo un dispositivo móvil utilizado sólo por usted y que esté apagado en el momento del robo.

Para no tener que introducir la contraseña cada vez que el sistema arranque y poder montar la partición codificada sólo cuando sea necesario, seleccione la opción 'No montar durante el inicio del sistema' en el diálogo 'Opciones fstab:'. La partición correspondiente se ignorará durante el arranque y deberá montarse explícitamente para poder acceder a ella: `mount` ⟨*`nombre_partición`*⟩ ⟨*`punto_montaje`*⟩. Después de introducir la contraseña, la partición será montada y podrá acceder a ella. Para impedir que otros usuarios tengan acceso a la misma, desmóntela con `umount nombre_partición` después de utilizarla.

Configuración de una partición codificada en el sistema activo

Aviso

Activar la codificación en el sistema activo

De manera similar al proceso descrito anteriormente para la instalación, es posible crear particiones codificadas mientras el sistema está en funcionamiento. No obstante, debe tener presente que, al codificar una partición ya disponible, todos los datos existentes se perderán.

Aviso

Seleccione en el sistema activo el módulo de YaST 'Particionador' a través del menú 'Sistema' del Centro de Control de YaST. Conteste 'Sí' a la pregunta de seguridad sobre el particionamiento en el sistema activo. A continuación se muestra una lista de todas las particiones disponibles. En lugar de 'Crear', pulse aquí 'Editar'. A partir de este punto, proceda como se describe en las líneas anteriores.

Creación de archivos codificados

Además de particiones enteras, también puede crear sistemas de archivos codificados basados en archivos para albergar sus datos confidenciales. Como en el caso de las particiones codificadas, el punto de partida es el diálogo de YaST 'Particionamiento en modo experto'. Seleccione la opción 'Archivo crypt' e introduzca en el siguiente diálogo la ruta al archivo y su tamaño. Acepte las opciones preseleccionadas correspondientes al formateado y por último defina si el sistema de archivos ha de montarse durante el arranque.

La ventaja de los archivos codificados reside en que pueden añadirse sin necesidad de modificar las particiones del disco duro. Se montan mediante un dispositivo de bucle y se manejan como particiones normales.

Codificación de archivos con vi

Un inconveniente de las particiones codificadas es que, mientras las particiones estén montadas, al menos el usuario `root` tiene acceso a los datos. Para evitarlo es posible utilizar el editor vi en modo codificado.

Ejecute el comando `vi -x nombre_archivo` para editar un nuevo archivo. Tras solicitar una contraseña, vi codificará el contenido del archivo. Cada vez que desee acceder a este archivo, vi le pedirá la contraseña.

Para obtener un máximo nivel de seguridad, puede guardar el archivo codificado en una partición cifrada. Esto puede resultar muy útil ya que el mecanismo criptográfico que utiliza vi no es muy seguro.

34.3.3. Codificar el contenido de medios extraíbles

Los medios extraíbles tales como los discos duros externos o los sticks USB son detectados por YaST de la misma forma que otros discos duros. Si desea codificar archivos o particiones en estos medios, proceda como se ha descrito arriba. En cualquier caso debe seleccionar la opción 'No montar durante el inicio del sistema' en el diálogo de 'Opciones fstab:', ya que este tipo de medios no suele estar disponible durante el arranque sino que se conecta posteriormente cuando el sistema está activo.

34.4. Seguridad y privacidad

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. En este contexto intervienen tanto aspectos de seguridad y como de 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 tiene como base una copia de seguridad periódica, funcional y comprobada. Sin la copia de seguridad de los archivos no sólo será difícil acceder a los datos en caso de un fallo del hardware sino en especial cuando exista la sospecha de que alguien ha tenido acceso a ciertos datos sin disponer de autorización.

34.4.1. Seguridad local y seguridad en la red

Existen diferentes formas de acceder a los datos:

- Comunicación directa con alguien que dispone de la información deseada o de acceso a determinados datos de un ordenador,
- 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 diferir algo en este aspecto, pero en cualquier caso seguro que nadie desea que el servidor de web revele sus datos personales a los internautas.

El primer punto de la lista es el más humano de todos. 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 este tipo contra el personal de recepción, el personal de servicio de la empresa o 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 la copia de seguridad 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 este hecho se pueden utilizar contraseñas para la BIOS y para el cargador de arranque.

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 archivo 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 satisface el nivel de seguridad 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 archivo 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 archivo 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 esta 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: EndlrdUE. Una contraseña del tipo Casanova o Lorena76 podría ser adivinada por alguien que le conozca más o menos bien.

El proceso de arranque

Para evitar que se pueda arrancar el sistema mediante un disquete o un CDROM, desmonte las unidades de lectura o seleccione una contraseña BIOS y determine en la BIOS que el arranque se realice exclusivamente desde el disco duro.

Los sistemas Linux arrancan generalmente con un cargador de arranque 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 que otorga desde un principio dichos permisos. Si utilizan GRUB como cargador de arranque, puede evitar esto introduciendo otra contraseña adicional en `/boot/grub/menu.lst` (ver capítulo ?? en esta página).

Permisos de acceso

Hay que partir del principio de que siempre se debe trabajar con el menor número de permisos posible. En definitiva, no es necesario estar registrado como usuario root para leer o escribir correo electrónico. Si el programa de correo (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 archivos que se distribuyen con SUSE se otorgan de forma cuidadosa. El administrador de un sistema sólo debería instalar software adicional u otros archivos con mucha precaución y siempre prestando atención especial a los derechos atribuidos a los archivos. 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 archivos 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 archivo pueda ser borrado o sobreescrito. Esto puede originar que los archivos intercambiados puedan ser ejecutados también por `root` o que los archivos 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 como ocurre con el cuco que hace que otros pájaros incuben sus huevos.

Los sistemas SUSE disponen de archivos `permissions`, `permissions.easy`, `permissions.secure` y `permissions.paranoid` en el directorio `/etc`. En estos archivos se determinan derechos especiales sobre archivos como por ejemplo directorios de escritura universal o setuser-ID-bits (el programa no se ejecuta con los permisos del propietario del proceso que lo ha arrancado sino con los permisos del propietario del archivo, que por norma general es `root`). El archivo `/etc/permissions.local` está a disposición del administrador; aquí podrá guardar sus propias modificaciones.

Para definir con comodidad cuáles son los archivos usados por los programas de configuración de SUSE para la adjudicación de los permisos existe el punto del menú 'Seguridad' de YaST. En el archivo `/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 estas bajo el control del usuario y no así del programador. Este es un error grave, especialmente cuando el programa se ejecuta con derechos especiales (ver la sección Permisos de acceso en esta página). Los llamados format string bugs funcionan de un modo algo distinto, pero utilizan igualmente datos de entrada del usuario para desviar el programa de su camino real.

Estos errores de programación son aprovechados 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 solo 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 anfitrión. Este anfitrión es un programa o un sector de memoria de importancia para el sistema, como por

ejemplo el MBR, al que debe tener acceso de escritura el código de programa del virus. Debido a sus características multiusuario, Linux puede limitar el derecho de escritura de los archivos, especialmente de los archivos 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 infectarse con un virus trabajando bajo Linux. Por otra parte, no debería ejecutar un programa que haya bajado de Internet y cuyo origen desconoce. La firma de los paquetes rpm de SUSE está codificada. 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 toman con seriedad suficiente 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 anfitrión 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 registrase 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 Window (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 de ventanas 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 (la pantalla) de accesos no autorizados. En este caso concreto, esto significa que el programa cliente tiene que recibir derechos. En X Window 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 pequeña base de datos en el servidor X. Pero limitarse a establecer una única autenticación 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 página man del comando `xhost` ofrece más explicaciones sobre el funcionamiento (y también contiene esta 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, las cuales contienen un papel con un proverbio en su interior) se graba en el archivo `.Xauthority` del directorio personal del usuario y de este modo, está a disposición de cualquier cliente de X Window que quiera abrir una ventana en el servidor X. El programa `xauth` ofrece al usuario la herramienta para explorar el archivo `.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 X Window le recomendamos la página man 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. Puede obtener información adicional sobre SSH en la sección **??** en esta página.

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 Window. Con el X11-forwarding conectado, los intrusos podrían autenticarse y conectarse con su servidor X a través de la conexión ssh y, por ejemplo, espiar el teclado.

Aviso

Buffer overflows y format string bugs

Lo dicho sobre buffer overflows y format string bugs en la sección Buffer overflows, format string bugs en esta página 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 código fuente 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 bloquear 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 percata 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 (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 anfitrión y su especialidad consiste en expandirse lo más rápidamente posible por la red. Algunos gusanos conocidos, como por ejemplo Ramen, Lion y Adore, utilizan 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 actualización. Naturalmente es requisito indispensable que el administrador del sistema instale las actualizaciones de seguridad en el sistema.

34.4.2. 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 instalar lo más rápidamente posible los paquetes de actualización anunciados 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.novell.com/linux/security/securitysupport.html`. `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 pueden resultar de utilidad:

- Evite trabajar como `root` siguiendo el principio de utilizar el mínimo privilegio posible para una tarea. Esto reduce las posibilidades de un huevo 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 basados únicamente 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 (por ejemplo bind, sendmail, ssh). Esto también es válido para la seguridad local.
- Optimice los derechos de acceso de los archivos del sistema que sean de importancia para la seguridad adaptando el archivo `/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 archivos 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 una copia de seguridad 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 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 paquete.rpm` muestra si la suma de control y la firma del paquete (¡no instalado!) coinciden. La clave se encuentra en el primer CD o DVD de SUSE LINUX y en la mayoría de los servidores de códigos (keyserver) del mundo.

- Compruebe regularmente las copias de seguridad de los datos y del sistema.

- Examine los archivos de registro o log files. Si es posible, debería escribir un pequeño script que se encargue de buscar entradas irregulares en estos archivos. 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 man de tcpd y `hosts_access` (`man tcpd`, `man hosts_access`) encontrará más información sobre `tcp_wrappern`.

- Utilice el cortafuegos de 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.

34.4.3. Notificación de nuevos problemas de seguridad

Si encuentra un problema de seguridad (después de haber comprobado los paquetes de actualización existentes), no dude en dirigirse a la dirección de correo electrónico `mailto: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 el mensaje con una codificación pgp. Nuestra clave pgp 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 descargar de `http://www.novell.com/linux/security/securitysupport.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.

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 borradores que se pueden consultar en la siguiente URL: `http://wt.xpilot.org/publications/posix.1e/`

35.1. ¿Por qué ACLs?

De manera tradicional, para cada objeto en Linux se definen 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 (owner), grupo (group) y el resto (other). Además es posible definir los bits *set user id*, *set group id* y *sticky*. 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, los administradores de sistemas debían echar mano antiguamente 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. Estas 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.

35.2. 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 (owner), grupo (group) y el resto de usuarios (other). Para cada clase de usuario se pueden definir otros tres bits de permisos (permission bits) para el derecho de lectura (`r`), de escritura (`w`) y de ejecución (`x`).

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 (ACL entries). Una entrada ACL consta de un tipo (ver la tabla **??** en esta página), 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.

35.3. Funcionamiento de las ACLs

La tabla **??** en esta página ofrece un resumen de los seis tipos posibles de entradas ACL, cada una de las cuales define un tipo de permisos para el propietario del archivo o directorio. La entrada *owning group* define los permisos del grupo propietario del archivo. El superusuario puede modificar el propietario o grupo propietario mediante el comando `chown` o `chgrp`, en cuyo caso el propietario y el grupo propietario se refieren al nuevo propietario y grupo propietario. Cada entrada *named user* define los permisos del usuario especificado en el campo cualificado correspondiente de la entrada (el campo situado en el centro del texto tal y como se muestra en la tabla ?? en esta página. Cada una de las entradas *named group* define los permisos del grupo especificado en el campo cualificado correspondiente de la entrada. Sólo las entradas named user y named group disponen de un campo cualificado que no está vacío. La entrada *other* define los permisos para el resto de usuarios.

mask limita aún más los permisos otorgados por las entradas *named user*, *named group* y *owning group*, ya que se emplea para especificar qué permisos son efectivos y cuáles están enmascarados en cada una de ellas. Si los permisos existen en una de las entradas mencionadas así como en la máscara, éstos son efectivos. Si, por el contrario, sólo están presentes en la máscara o en la entrada, no lo son, por lo que no se aplican. Todos los permisos contenidos en las entradas *owner* y *owning group* siempre tienen vigencia. Este esquema se explica en la tabla **??** en esta página.

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* (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 ?? en esta página ofrece un resumen de los distintos tipos de entradas ACL.

Cuadro 35.1: *Resumen de tipos de entrada 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 35.2: *Enmascaramiento de permisos de acceso*

Tipo	**Formato en texto**	**Permisos**
named user	`user:geeko:r-x`	`r-x`
mask	`mask::rw-`	`rw-`
	permisos efectivos:	`r--`

35.3.1. Entradas ACL y bits de permiso

Los siguientes gráficos ilustran respectivamente las posibles variantes de una ACL estándar y una extendida (ver figura **??** en esta página y figura **??** en esta página). 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.

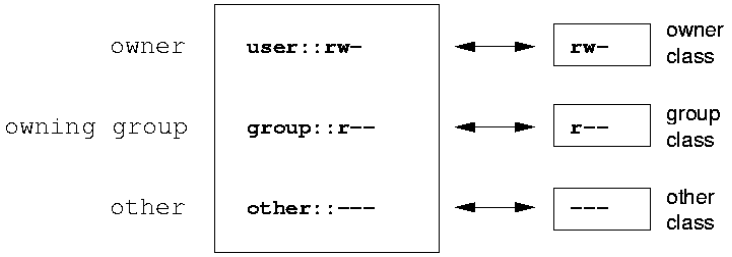

Figura 35.1: *ACL estándar: entradas ACL y bits de permiso*

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 figura ?? en esta página). En el caso de una ACL extendida (con entrada *mask*), los permisos de la *group class* se asignan a la entrada *mask* (ver figura ?? en esta página).

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 y viceversa.

35.3.2. Un directorio con access ACL

Por medio del siguiente ejemplo, se explicará en tres pasos el funcionamiento de una access ACL:

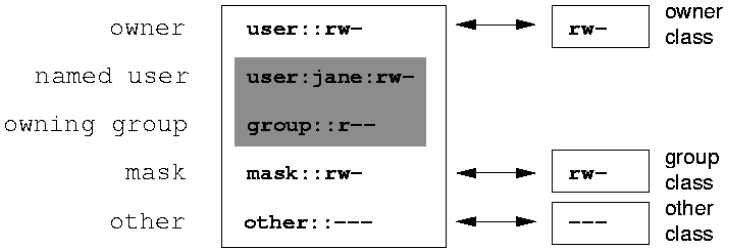

Figura 35.2: *ACL extendida: entradas ACL y bits de permiso*

Antes de crear un directorio, puede emplear el comando `umask` para definir qué permisos de acceso han de estar enmascarados desde el momento de su creación. `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`).

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`. La salida en este caso sería:

```
drwxr-x--- ... tux project3 ... mydir
```

Mediante el comando `getfacl mydir` puede comprobar el estado inicial de la ACL:

```
# file: mydir
# owner: tux
# group: project3
user::rwx
group::r-x
other::---
```

La salida del comando `getfacl` refleja exactamente la correspondencia entre bits de permiso y entradas ACL descrita en la sección **??** en esta página. 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 `geeko` y a un nuevo grupo `mascots` permisos de lectura, escritura y ejecución.

```
setfacl -m user:geeko:rwx,group:mascots: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`.

```
# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx
group::r-x
group:mascots:rwx
mask::rwx
other::---
```

Además de las entradas para el usuario `geeko` y el grupo `mascots` 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 estas 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`.

```
drwxrwx---+ ... tux project3 ... 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: `project3`) tendría asimismo derechos de escritura para el directorio `mydir`. No obstante, los permisos de acceso realmente válidos para 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 ?? en esta página). 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`. Por ejemplo, emplee el comando `chmod g-w mydir`. `ls -dl mydir` muestra lo siguiente:

```
drwxr-x---+ ... tux project3 ... mydir
```

`getfacl mydir` ofrece la siguiente salida:

```
# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx          # effective: r-x
group::r-x
group:mascots:rwx      # effective: r-x
mask::r-x
other::---
```

Después de 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:

35.3.3. Directorios con ACLs predeterminadas

Los directorios pueden ser equipados con un tipo especial de ACLs, las ACLs predeterminadas. Estas definen los derechos que heredan 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 (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. En este caso no se tiene 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:

1. A continuación se añade una ACL predeterminada al directorio `mydir` ya existente:

   ```
   setfacl -d -m group:mascots: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: project3
   user::rwx
   user:geeko:rwx
   group::r-x
   group:mascots:rwx
   ```

```
mask::rwx
other::---
default:user::rwx
default:group::r-x
default:group:mascots:r-x
default:mask::r-x
default:other::---
```

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 `mascots` en la ACL predeterminada, `setfacl` ha copiado automáticamente el resto de entradas del 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: project3
user::rwx
group::r-x
group:mascots:r-x
mask::r-x
other::---
default:user::rwx
default:group::r-x
default:group:mascots:r-x
default:mask::r-x
default:other::---
```

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`, por ejemplo, `touch mydir/myfile`. `ls -l mydir/myfile` genera la salida:

```
-rw-r-----+ ... tux project3 ... mydir/myfile
```

La salida del comando `getfacl mydir/myfile` es:

```
# file: mydir/myfile
# owner: tux
# group: project3
user::rw-
group::r-x          # effective:r--
group:mascots: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 esta página). 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 puedan ejecutar los archivos.

35.3.4. 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.

35.4. Soporte en aplicaciones

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. Los comandos de archivos básicos (`cp`, `mv`, `ls`, etc.) soportan las ACLs así como Samba.

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. En el campo de los programas de copias de seguridad, no existe (con la excepción del archivador star) ningún programa que pueda garantizar el mantenimiento total de las ACLs.

35.5. Información adicional

Puede encontrar información detallada (en inglés) sobre las ACLs en `http://acl.bestbits.at/`.

Asimismo, le recomendamos que consulte las páginas de manual de `getfacl(1)`, `acl(5)` y `setfacl(1)`

Herramientas de vigilancia del sistema

En este capítulo se presentan distintos comandos y procedimientos mediante los cuales puede analizarse el estado del sistema. Además se describen varias herramientas junto con sus opciones más importantes que pueden resultar de utilidad en el trabajo diario.

Cada vez que se comenta un comando, se incluye su correspondiente salida en pantalla. La primera línea corresponde al comando en sí (ubicado tras el carácter que representa la línea de comandos, en este caso el signo del dólar). Los fragmentos omitidos se indican mediante corchetes (`[...]`) y, si es necesario, se dividen las líneas demasiado extensas. Esta división se simboliza mediante una barra inversa (\):

```
$ command -x -y
output line 1
output line 2
output line 3 is annoyingly long, so long that \
    we have to break it
output line 3
[...]
output line 98
output line 99
```

Asimismo, se adjunta una descripción concisa de cada comando en la que se incluye un resumen de todas sus funciones. Puede encontrar información más detallada acerca de los comandos en las páginas del manual correspondientes. La mayoría de comandos admite también el parámetro `--help`, mediante el cual podrá visualizar una lista de todas las opciones posibles.

36.1. Listado de los archivos abiertos: lsof

Si desea visualizar el listado de todos los archivos que mantiene abiertos un determinado ID de proceso (⟨*PID*⟩), puede utilizar la opción `-p`. Por ejemplo, para mostrar todos los archivos utilizados por la shell actual, ejecute:

```
$ lsof -p $$
COMMAND  PID USER   FD   TYPE DEVICE    SIZE     NODE NAME
zsh     4694   jj  cwd    DIR   0,18     144 25487368 /suse/jj/t (totan:/real-home/jj)
zsh     4694   jj  rtd    DIR    3,2     608        2 /
zsh     4694   jj  txt    REG    3,2  441296    20414 /bin/zsh
zsh     4694   jj  mem    REG    3,2  104484    10882 /lib/ld-2.3.3.so
zsh     4694   jj  mem    REG    3,2   11648    20610 /usr/lib/zsh/4.2.0/zsh/rlimits.so
[...]
zsh     4694   jj  mem    REG    3,2   13647    10891 /lib/libdl.so.2
zsh     4694   jj  mem    REG    3,2   88036    10894 /lib/libnsl.so.1
zsh     4694   jj  mem    REG    3,2  316410   147725 /lib/libncurses.so.5.4
zsh     4694   jj  mem    REG    3,2  170563    10909 /lib/tls/libm.so.6
zsh     4694   jj  mem    REG    3,2 1349081    10908 /lib/tls/libc.so.6
zsh     4694   jj  mem    REG    3,2      56    12410 /usr/lib/locale/de_DE.utf8/LC_TELEPHONE
[...]
zsh     4694   jj  mem    REG    3,2      59    14393 /usr/lib/locale/en_US/LC_NUMERIC
zsh     4694   jj  mem    REG    3,2  178476    14565 /usr/lib/locale/en_US/LC_CTYPE
zsh     4694   jj  mem    REG    3,2   56444    20598 /usr/lib/zsh/4.2.0/zsh/computil.so
```

```
zsh     4694   jj    0u   CHR 136,48              50 /dev/pts/48
zsh     4694   jj    1u   CHR 136,48              50 /dev/pts/48
zsh     4694   jj    2u   CHR 136,48              50 /dev/pts/48
zsh     4694   jj   10u   CHR 136,48              50 /dev/pts/48
```

En el ejemplo se ha utilizado la variable `$$`, cuyo valor es el ID de proceso de la shell.

Si no se indica ninguna opción, `lsof` enumera todos los archivos abiertos en ese momento. Puesto que no es raro que haya miles de archivos abiertos, una lista de todos ellos no suele resultar de utilidad. No obstante, es posible combinar la lista de todos los archivos con funciones de búsqueda para generar listas útiles, como por ejemplo un listado de todos los dispositivos de caracteres (character devices) utilizados:

```
$ lsof | grep CHR
sshd       4685    root  mem    CHR    1,5            45833 /dev/zero
sshd       4685    root  mem    CHR    1,5            45833 /dev/zero
sshd       4693      jj  mem    CHR    1,5            45833 /dev/zero
sshd       4693      jj  mem    CHR    1,5            45833 /dev/zero
zsh        4694      jj    0u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj    1u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj    2u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj   10u   CHR 136,48               50 /dev/pts/48
X          6476    root  mem    CHR    1,1            38042 /dev/mem
lsof      13478      jj    0u   CHR 136,48               50 /dev/pts/48
lsof      13478      jj    2u   CHR 136,48               50 /dev/pts/48
grep      13480      jj    1u   CHR 136,48               50 /dev/pts/48
grep      13480      jj    2u   CHR 136,48               50 /dev/pts/48
```

36.2. Usuario que accede a los archivos: fuser

En ocasiones puede resultar práctico saber qué procesos o usuarios están accediendo a ciertos archivos en ese momento. Supongamos por ejemplo que desea desmontar un sistema de archivos montado en `/mnt` pero el comando `umount` devuelve el mensaje "device is busy." En este caso, el comando `fuser` puede emplearse para determinar qué procesos están accediendo al dispositivo:

```
$ fuser -v /mnt/*

                     USER        PID ACCESS COMMAND
/mnt/notes.txt
                     jj        26597 f....  less
```

El sistema de archivos puede desmontarse cuando finalice el proceso `less`, el cual estaba siendo ejecutado desde otro terminal.

36.3. Propiedades de un archivo: stat

El comando `stat` muestra las propiedades de un archivo:

```
$ stat xml-doc.txt
  File: ‘xml-doc.txt’
  Size: 632             Blocks: 8          IO Block: 4096   regular file
Device: eh/14d  Inode: 5938009     Links: 1
Access: (0644/-rw-r--r--)  Uid: (11994/      jj)   Gid: (   50/    suse)
Access: 2004-04-27 20:08:58.000000000 +0200
Modify: 2003-06-03 15:29:34.000000000 +0200
Change: 2003-07-23 17:48:27.000000000 +0200
```

Mediante el parámetro `--filesystem` se muestran las características del sistema de archivos en el que se encuentra almacenado el archivo:

```
$ stat  . --filesystem
  File: "."
    ID: 0        Namelen: 255     Type: ext2/ext3
Blocks: Total: 19347388   Free: 17831731   Available: 16848938   Size: 4096
Inodes: Total: 9830400    Free: 9663967
```

En caso de que utilice z-shell (`zsh`), debe introducir `/usr/bin/stat`. Esto se debe a que z-shell dispone de un `stat` integrado con opciones y formato de salida diferentes:

```
% type stat
stat is a shell builtin
% stat .
device  769
inode   4554808
mode    16877
nlink   12
uid     11994
gid     50
rdev    0
size    4096
atime   1091536882
mtime   1091535740
ctime   1091535740
blksize 4096
blocks  8
link
```

36.4. Dispositivos USB: lsusb

El comando `lsusb` proporciona una lista de todos los dispositivos USB. La opción `-v` le permite imprimir una lista más detallada que se lee del directorio `/proc/bus/usb/`. A continuación se muestra la salida de `lsusb` después de conectar un stick de memoria USB. Las últimas líneas alertan de la presencia del nuevo dispositivo.

```
Bus 004 Device 001: ID 0000:0000
Bus 003 Device 001: ID 0000:0000
Bus 002 Device 001: ID 0000:0000
Bus 001 Device 001: ID 0000:0000
Bus 001 Device 018: ID 0402:5634 ALi Corp.
```

36.5. Información sobre un dispositivo SCSI: scsiinfo

El comando `scsiinfo` muestra información sobre un dispositivo SCSI. La opción `-l` proporciona una lista con todos los dispositivos SCSI conocidos en el sistema (el comando `lsscsi` facilita información similar). A continuación se incluye la salida de `scsiinfo -i /dev/sda` que contiene información acerca de un disco duro. La opción `-a` aumenta la cantidad de información mostrada.

```
Inquiry command
---------------
Relative Address                  0
Wide bus 32                       0
Wide bus 16                       1
Synchronous neg.                  1
Linked Commands                   1
Command Queueing                  1
SftRe                             0
Device Type                       0
Peripheral Qualifier              0
Removable?                        0
Device Type Modifier              0
ISO Version                       0
ECMA Version                      0
```

```
ANSI Version                        3
AENC                                0
TrmIOP                              0
Response Data Format                2
Vendor:                     FUJITSU
Product:                    MAS3367NP
Revision level:             0104A0K7P43002BE
```

Existen dos listas de bloques defectuosos en el disco duro: la primera está elaborada por el fabricante (manufacturer table) y la segunda recoge los bloques defectuosos aparecidos durante la operación (grown table). Si el número de entradas en grown table aumenta, se recomienda cambiar el disco duro.

36.6. Mostrar procesos: top

El comando `top` (table of processes) proporciona una lista de los procesos en ejecución. Este listado se actualiza cada 2 segundos. Para salir, pulse Q. La opción `-n 1` cierra el programa tras mostrar la lista de procesos una sola vez. A continuació se muestra un ejemplo de la salida de `top -n 1`:

```
$ top -n 1
top - 14:19:53 up 62 days,  3:35, 14 users,  load average: 0.01, 0.02, 0.00
Tasks: 102 total,   7 running,  93 sleeping,   0 stopped,   2 zombie
Cpu(s):   0.3% user,   0.1% system,   0.0% nice,  99.6% idle
Mem:    514736k total,   497232k used,    17504k free,    56024k buffers
Swap:  1794736k total,   104544k used,  1690192k free,   235872k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  Command
 1426 root      15   0  116m  41m  18m S  1.0  8.2  82:30.34 X
20836 jj        15   0   820  820  612 R  1.0  0.2   0:00.03 top
    1 root      15   0   100   96   72 S  0.0  0.0   0:08.43 init
    2 root      15   0     0    0    0 S  0.0  0.0   0:04.96 keventd
    3 root      34  19     0    0    0 S  0.0  0.0   0:00.99 ksoftirqd_CPU0
    4 root      15   0     0    0    0 S  0.0  0.0   0:33.63 kswapd
    5 root      15   0     0    0    0 S  0.0  0.0   0:00.71 bdflush
      [...]
 1362 root      15   0   488  452  404 S  0.0  0.1   0:00.02 nscd
 1363 root      15   0   488  452  404 S  0.0  0.1   0:00.04 nscd
 1377 root      17   0    56    4    4 S  0.0  0.0   0:00.00 mingetty
 1379 root      18   0    56    4    4 S  0.0  0.0   0:00.01 mingetty
 1380 root      18   0    56    4    4 S  0.0  0.0   0:00.01 mingetty
```

Si el proceso `top` se encuentra activo, puede pulsar la tecla F para acceder a un menú desde el que puede modificarse el formato de salida.

Para controlar únicamente los procesos pertenecientes a un determinado usuario, emplee la opción `-U UID`, donde ⟨*UID*⟩ es el ID de usuario. El comando `top -U $(id -u nombre_usuario)` se averigua el UID del usuario por medio del nombre de usuario y se muestra una lista con sus procesos.

36.7. Mostrar lista de procesos: ps

El comando `ps` presenta en pantalla la lista completa de procesos. Con la opción `r` se muestran los que están consumiendo tiempo de cálculo en ese momento:

```
$ ps r
  PID TTY      STAT   TIME COMMAND
22163 pts/7    R      0:01 -zsh
 3396 pts/3    R      0:03 emacs new-makedoc.txt
20027 pts/7    R      0:25 emacs xml/common/utilities.xml
20974 pts/7    R      0:01 emacs jj.xml
27454 pts/7    R      0:00 ps r
```

Observe que el parámetro ha de indicarse sin emplear el signo menos. Algunas opciones utilizan el signo menos y otras no. Si desea obtener más información al respecto, consulte la página del manual correspondiente. Si el aspecto de la página man le resulta algo complejo, puede utilizar `ps --help` para visualizar en pantalla una breve descripción del comando.

Para controlar cuántos procesos `emacs` están activos utilice:

```
$ ps x | grep emacs
 1288 ?        S      0:07 emacs
 3396 pts/3    S      0:04 emacs new-makedoc.txt
 3475 ?        S      0:03 emacs .Xresources
20027 pts/7    S      0:40 emacs xml/common/utilities.xml
20974 pts/7    S      0:02 emacs jj.xml

$ pidof emacs
20974 20027 3475 3396 1288
```

Mediante el parámetro `-p` se ordenan los procesos según su ID:

```
$ ps www -p $(pidof xterm)
  PID TTY      STAT   TIME COMMAND
```

```
 9025 ?        S      0:01 xterm -g 100x45+0+200
 9176 ?        S      0:00 xterm -g 100x45+0+200
29854 ?        S      0:21 xterm -g 100x75+20+0 -fn \
  -B&H-LucidaTypewriter-Medium-R-Normal-Sans-12-120-75-75-M-70-iso10646-1
 4378 ?        S      0:01 xterm -bg MistyRose1 -T root -n root -e su -l
25543 ?        S      0:02 xterm -g 100x45+0+200
22161 ?        R      0:14 xterm -g 100x45+0+200
16832 ?        S      0:01 xterm -bg MistyRose1 -T root -n root -e su -l
16912 ?        S      0:00 xterm -g 100x45+0+200
17861 ?        S      0:00 xterm -bg DarkSeaGreen1 -g 120x45+40+300
19930 ?        S      0:13 xterm -bg LightCyan
21686 ?        S      0:04 xterm -g 100x45+0+200 -fn \
lucidasanstypewriter-12
23104 ?        S      0:00 xterm -g 100x45+0+200
26547 ?        S      0:00 xterm -g 100x45+0+200
```

La lista de procesos puede formatearse en función de las necesidades del usuario. La opción `-L` produce una lista de todas las palabras clave. Si desea una lista de todos los procesos ordenados según su consumo de memoria, ejecute el comando:

```
$ ps ax --format pid,rss,cmd --sort rss
  PID  RSS CMD
    2    0 [ksoftirqd/0]
    3    0 [events/0]
   17    0 [kblockd/0]
[...]
10164 5260 xterm
31110 5300 xterm
17010 5356 xterm
 3896 29292 /usr/X11R6/bin/X -nolisten tcp -br vt7 -auth /var/lib/xdm/authdir/au
```

36.8. Mostrar el árbol de procesos: pstree

El comando `pstree` muestra en pantalla la lista de procesos siguiendo una estructura de árbol:

```
$ pstree
init-+-atd
     |-3*[automount]
```

```
    |-bdflush
    |-cron
  [...]
    |-usb-storage-1
    |-usb-storage-2
    |-10*[xterm---zsh]
    |-xterm---zsh---mutt
    |-2*[xterm---su---zsh]
    |-xterm---zsh---ssh
    |-xterm---zsh---pstree
    |-ypbind---ypbind---2*[ypbind]
    `-zsh---startx---xinit4-+-X
                            `-ctwm-+-xclock
                                   |-xload
                                   `-xosview.bin
```

Si utiliza la opción `-p`, el ID de proceso se incluye junto al nombre. Asimismo, es posible mostrar también los argumentos de la línea de comando a través del parámetro `-a`:

```
$ pstree -pa
init,1
  |-atd,1255
[...]
  `-zsh,1404
      `-startx,1407 /usr/X11R6/bin/startx
          `-xinit4,1419 /suse/jj/.xinitrc [...]
              |-X,1426 :0 -auth /suse/jj/.Xauthority
              `-ctwm,1440
                  |-xclock,1449 -d -geometry -0+0 -bg grey
                  |-xload,1450 -scale 2
                  `-xosview.bin,1451 +net -bat +net
```

36.9. Mostrar quién hace qué: w

El comando `w` se emplea para determinar quién dispone de una sesión activa y qué procesos tiene abiertos. Ejemplo:

```
$ w
 15:17:26 up 62 days,  4:33, 14 users,  load average: 0.00, 0.04, 0.01
USER     TTY        LOGIN@   IDLE   JCPU   PCPU WHAT
jj       pts/0     30Mar04  4days  0.50s  0.54s xterm -bg MistyRose1 -e su -l
jj       pts/1     23Mar04  5days  0.20s  0.20s -zsh
```

```
jj       pts/2     23Mar04  5days  1.28s  1.28s -zsh
jj       pts/3     23Mar04  3:28m  3.21s  0.50s -zsh
[...]
jj       pts/7     07Apr04  0.00s  9.02s  0.01s w
jj       pts/9     25Mar04  3:24m  7.70s  7.38s mutt
[...]
jj       pts/14    12:49   37:34   0.20s  0.13s ssh totan
```

La última línea revela que el usuario jj ha establecido una conexión shell segura (`ssh`) con el ordenador `totan`. En el caso de que algún usuario haya iniciado una sesión remota desde otro sistema, es posible emplear el parámetro `-f` para conocer de qué ordenador se trata.

36.10. Mostrar el consumo de memoria: free

El nivel de utilización de la memoria RAM se analiza mediante la herramienta `free`. Este comando muestra tanto la memoria física como la de intercambio (swap) libre y ocupada:

```
$ free
             total       used       free     shared    buffers     cached
Mem:        514736     273964     240772          0      35920      42328
-/+ buffers/cache:     195716     319020
Swap:      1794736     104096    1690640
```

Utilice la opción `-m` para visualizar todos los valores en megabytes:

```
$ free -m
             total       used       free     shared    buffers     cached
Mem:           502        267        235          0         35         41
-/+ buffers/cache:        191        311
Swap:         1752        101       1651
```

La información realmente interesante se encuentra en la siguiente línea:

```
-/+ buffers/cache:        191        311
```

Aquí se muestra el nivel de utilización por parte del búfer y la caché. Emplee la opción `-d N` para establecer la frecuencia de actualización en ⟨*N*⟩ segundos con la que se mostrará la información: `free -d 1.5` actualiza los datos cada 1,5 segundos.

36.11. Kernel Ring Buffer: dmesg

El kernel de Linux almacena un número determinado de mensajes de sistema en una área denominada Ring Buffer. El comando `dmesg` se emplea para mostrar estos mensajes:

```
$ dmesg
[...]
sdc : READ CAPACITY failed.
sdc : status = 1, message = 00, host = 0, driver = 08
Info fld=0xa00 (nonstd), Current sd00:00: sense key Not Ready
sdc : block size assumed to be 512 bytes, disk size 1GB.
sdc: test WP failed, assume Write Enabled
 sdc: I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 2097144
 I/O error: dev 08:20, sector 2097144
 I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 0
 unable to read partition table
 I/O error: dev 08:20, sector 0
nfs: server totan not responding, still trying
nfs: server totan OK
```

La penúltima línea indica la existencia de un problema temporal con el servidor NFS `totan`. Las líneas anteriores han sido generadas debido a que el usuario ha conectado en el ordenador un dispositivo USB de memoria. Los eventos anteriores quedan registrados en los archivos `/var/log/messages` y `/var/log/warn`.

36.12. Sistemas de archivos: mount, df y du

Mediante `mount` se determina qué sistema de archivos (dispositivo y tipo) está montado y en qué punto (mount point):

```
$ mount
/dev/hdb2 on / type ext2 (rw)
proc on /proc type proc (rw)
```

```
devpts on /dev/pts type devpts (rw,mode=0620,gid=5)
/dev/hda1 on /data type ext2 (rw)
shmfs on /dev/shm type shm (rw)
usbdevfs on /proc/bus/usb type usbdevfs (rw)
automount(pid1012) on /suse type autofs \
    (rw,fd=5,pgrp=1012,minproto=2,maxproto=3)
totan:/real-home/jj on /suse/jj type nfs \
    (rw,nosuid,rsize=8192,wsize=8192,hard,intr,nolock,addr=10.10.0.1)
```

Si desea visualizar un resumen acerca del nivel de utilización del sistema de archivos, emplee la instrucción `df`. La opción `-h` (alias `--human-readable`) indica al comando que la información sea presentada de forma comprensible para el usuario:

```
$ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/hdb2             7.4G  5.1G  2.0G  73% /
/dev/hda1              74G  5.8G   65G   9% /data
shmfs                 252M     0  252M   0% /dev/shm
totan:/real-home/jj   350G  324G   27G  93% /suse/jj
```

El usuario del servidor de archivos NFS `totan` debería llevar a cabo una limpieza urgente de su directorios home. Con la ayuda del comando `du`, puede determinarse el tamaño total de todos los archivos contenidos en un directorio. La opción `-s` simplifica el tipo de información presentada en pantalla mientras que el parámetro `-h` la hace comprensible para el usuario.

Mediante

```
$ du -sh ~
361M    /suse/jj
```

puede averiguar cuánto espacio ocupa el directorio home del usuario.

36.13. El sistema de archivos /proc

`/proc` es una especie de sistema de archivos utilizado por el kernel para almacenar información importante acerca del sistema en forma de archivos virtuales. Por ejemplo, es posible conocer el tipo de procesador ejecutando el siguiente comando:

```
$ cat /proc/cpuinfo
processor       : 0
vendor_id       : AuthenticAMD
cpu family      : 6
model           : 8
model name      : AMD Athlon(tm) XP 2400+
stepping        : 1
cpu MHz         : 2009.343
cache size      : 256 KB
fdiv_bug        : no
[...]
```

Asimismo, puede visualizarse qué interrupciones se encuentran ocupadas:

```
$ cat /proc/interrupts
           CPU0
  0:  537544462          XT-PIC  timer
  1:     820082          XT-PIC  keyboard
  2:          0          XT-PIC  cascade
  8:          2          XT-PIC  rtc
  9:          0          XT-PIC  acpi
 10:      13970          XT-PIC  usb-uhci, usb-uhci
 11:  146467509          XT-PIC  ehci_hcd, usb-uhci, eth0
 12:    8061393          XT-PIC  PS/2 Mouse
 14:    2465743          XT-PIC  ide0
 15:       1355          XT-PIC  ide1
NMI:          0
LOC:          0
ERR:          0
MIS:          0
```

A continuación se muestra una lista con algunos de los archivos que contienen información relevante acerca del sistema:

`/proc/devices` dispositivos disponibles

`/proc/modules` módulos del kernel cargados

`/proc/cmdline` línea de comandos del kernel

`/proc/meminfo` información detallada acerca del nivel de utilización de la memoria

`/proc/config.gz` archivo actual de configuración del kernel comprimido mediante `gzip`

Asimismo, puede obtener información adicional en el archivo de texto: `/usr/src/linux/Documentation/filesystems/proc.txt`. La información referente a los procesos activos se encuentra ubicada en los directorios `/proc/`⟨*NNN*⟩, donde ⟨*NNN*⟩ es el ID del proceso correspondiente (PID). Todos los procesos pueden encontrar sus propias características en `/proc/self/`:

```
$ ls -l /proc/self
lrwxrwxrwx  1 root root 64 Apr 29 13:52 /proc/self -> 27585

$ ls -l /proc/self/
total 0
dr-xr-xr-x  2 jj suse 0 Apr 29 13:52 attr
-r--------  1 jj suse 0 Apr 29 13:52 auxv
-r--r--r--  1 jj suse 0 Apr 29 13:52 cmdline
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 cwd -> /suse/jj/t
-r--r--r--  1 jj suse 0 Apr 29 13:52 delay
-r--------  1 jj suse 0 Apr 29 13:52 environ
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 exe -> /bin/ls
dr-x------  2 jj suse 0 Apr 29 13:52 fd
-rw-------  1 jj suse 0 Apr 29 13:52 mapped_base
-r--r--r--  1 jj suse 0 Apr 29 13:52 maps
-rw-------  1 jj suse 0 Apr 29 13:52 mem
-r--r--r--  1 jj suse 0 Apr 29 13:52 mounts
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 root -> /
-r--r--r--  1 jj suse 0 Apr 29 13:52 stat
-r--r--r--  1 jj suse 0 Apr 29 13:52 statm
-r--r--r--  1 jj suse 0 Apr 29 13:52 status
dr-xr-xr-x  3 jj suse 0 Apr 29 13:52 task
-r--r--r--  1 jj suse 0 Apr 29 13:52 wchan
```

El archivo `maps` alberga la tabla de direccionamiento de ejecutables y librerías:

```
$ cat /proc/self/maps
08048000-0804c000 r-xp 00000000 03:02 22890      /bin/cat
0804c000-0804d000 rw-p 00003000 03:02 22890      /bin/cat
0804d000-0806e000 rwxp 0804d000 00:00 0
40000000-40016000 r-xp 00000000 03:02 10882      /lib/ld-2.3.3.so
40016000-40017000 rw-p 00015000 03:02 10882      /lib/ld-2.3.3.so
40017000-40018000 rw-p 40017000 00:00 0
4002b000-40135000 r-xp 00000000 03:02 10908      /lib/tls/libc.so.6
40135000-4013d000 rw-p 0010a000 03:02 10908      /lib/tls/libc.so.6
4013d000-40141000 rw-p 4013d000 00:00 0
bfffe000-c0000000 rw-p bfffe000 00:00 0
ffffe000-fffff000 ---p 00000000 00:00 0
```

36.14. vmstat, iostat y mpstat

La herramienta `vmstat` proporciona estadísticas de la memoria virtual. Dicha herramienta evalúa los archivos `/proc/meminfo`, `/proc/stat` y `/proc/*/`

`stat` y resulta muy útil para identificar "cuellos de botella" en el rendimiento del sistema. El comando `iostat` ofrece estadísticas sobre la CPU y datos de salida y entrada para dispositivos y particiones. La información mostrada se toma de los archivos `/proc/stat` y `/proc/partitions`. El resultado de este comando puede utilizarse para equilibrar mejor la carga de entrada y de salida entre discos duros. El comando `mpstat` muestra también datos estadísticos relacionados con la CPU.

36.15. procinfo

La herramienta `procinfo` muestra en pantalla información procedente del directorio `/proc`:

```
$ procinfo
Linux 2.6.4-54.5-default (geeko@buildhost) (gcc 3.3.3 ) #1 1CPU [roth.suse.de]


Memory:      Total        Used        Free      Shared     Buffers
Mem:        516696      513200        3496           0       43284
Swap:       530136        1352      528784

Bootup: Wed Jul  7 14:29:08 2004    Load average: 0.07 0.04 0.01 1/126 5302

user  :       2:42:28.08   1.3%  page in :        0
nice  :       0:31:57.13   0.2%  page out:        0
system:       0:38:32.23   0.3%  swap in :        0
idle  :   3d 19:26:05.93  97.7%  swap out:        0
uptime:   4d  0:22:25.84         context :207939498

irq  0: 776561217 timer               irq  8:         2 rtc
irq  1:    276048 i8042               irq  9:     24300 VIA8233
irq  2:         0 cascade [4]         irq 11:  38610118 acpi, eth0, uhci_hcd
irq  3:         3                     irq 12:   3435071 i8042
irq  4:         3                     irq 14:   2236471 ide0
irq  6:         2                     irq 15:       251 ide1
```

Si necesita visualizar "toda" la información disponible, utilice la opción `-a`. Mediante el parámetro `-nN`, es posible especificar la frecuencia de actualización en $\langle N \rangle$ segundos. Para abandonar la herramienta, emplee la tecla Q.

Por defecto se muestran los valores totales acumulados. Si se emplea la opción `-d`, se indican los valores parciales: `procinfo -dn5` muestra los valores actualizados cada 5 segundos:

```
Memory:      Total        Used        Free      Shared     Buffers      Cached
Mem:             0           2          -2           0           0           0
Swap:            0           0           0

Bootup: Wed Feb 25 09:44:17 2004    Load average: 0.00 0.00 0.00 1/106 31902

user  :       0:00:00.02   0.4%  page in :        0  disk 1:        0r       0w
nice  :       0:00:00.00   0.0%  page out:        0  disk 2:        0r       0w
system:       0:00:00.00   0.0%  swap in :        0  disk 3:        0r       0w
idle  :       0:00:04.99  99.6%  swap out:        0  disk 4:        0r       0w
uptime:  64d  3:59:12.62         context :     1087

irq  0:       501 timer               irq 10:         0 usb-uhci, usb-uhci
irq  1:         1 keyboard            irq 11:        32 ehci_hcd, usb-uhci,
irq  2:         0 cascade [4]         irq 12:       132 PS/2 Mouse
irq  6:         0                     irq 14:         0 ide0
irq  8:         0 rtc                 irq 15:         0 ide1
irq  9:         0 acpi
```

36.16. Recursos PCI: lspci

El comando `lspci` enumera los recursos PCI:

```
$ lspci
00:00.0 Host bridge: VIA Technologies, Inc. \
    VT8366/A/7 [Apollo KT266/A/333]
00:01.0 PCI bridge: VIA Technologies, Inc. \
    VT8366/A/7 [Apollo KT266/A/333 AGP]
00:0b.0 Ethernet controller: Digital Equipment Corporation \
    DECchip 21140 [FasterNet] (rev 22)
00:10.0 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.1 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.2 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.3 USB Controller: VIA Technologies, Inc. USB 2.0 (rev 82)
00:11.0 ISA bridge: VIA Technologies, Inc. VT8235 ISA Bridge
00:11.1 IDE interface: VIA Technologies, Inc. VT82C586/B/686A/B \
    PIPC Bus Master IDE (rev 06)
00:11.5 Multimedia audio controller: VIA Technologies, Inc. \
    VT8233 AC97 Audio Controller (rev 50)
01:00.0 VGA compatible controller: Matrox Graphics, Inc. \
    MGA G550 AGP (rev 01)
```

Si desea obtener una lista más detallada, utilice el parámetro `-v`:

```
$ lspci -v
[...]
01:00.0 \
 VGA compatible controller: Matrox Graphics, Inc. MGA G550 AGP (rev 01) \
```

```
   (prog-if 00 [VGA])
Subsystem: Matrox Graphics, Inc. Millennium G550 Dual Head DDR 32Mb
Flags: bus master, medium devsel, latency 32, IRQ 10
Memory at d8000000 (32-bit, prefetchable) [size=32M]
Memory at da000000 (32-bit, non-prefetchable) [size=16K]
Memory at db000000 (32-bit, non-prefetchable) [size=8M]
Expansion ROM at <unassigned> [disabled] [size=128K]
Capabilities: <available only to root>
```

La resolución de nombres de los dispositivos se realiza por medio del archivo `/usr/share/pci.ids`. Los IDs de los dispositivos PCI que no se encuentren almacenados en este archivo se mostrarán como "Unknown device".

La opción `-vv` se emplea para poder visualizar toda la información disponible. Si desea obtener simplemente los códigos numéricos, emplee la opción `-n`.

36.17. Llamadas al sistema: strace

Todas las llamadas al sistema originadas por un proceso pueden ser rastreadas mediante la herramienta `strace`. Para ello, introduzca el comando del modo habitual añadiendo `strace` al principio de la expresión:

```
$ strace -e open ls

execve("/bin/ls", ["ls"], [/* 88 vars */]) = 0
uname({sys="Linux", node="edison", ...}) = 0
brk(0)                                  = 0x805b000
old_mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
        = 0x40017000
open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=76333, ...}) = 0
old_mmap(NULL, 76333, PROT_READ, MAP_PRIVATE, 3, 0) = 0x40018000
[...]
ioctl(1, SNDCTL_TMR_TIMEBASE or TCGETS, {B38400 opost isig icanon echo ...}) = 0
ioctl(1, TIOCGWINSZ, {ws_row=53, ws_col=110, ws_xpixel=897, ws_ypixel=693}) = 0
open(".", O_RDONLY|O_NONBLOCK|O_LARGEFILE|O_DIRECTORY) = 3
fstat64(3, {st_mode=S_IFDIR|0755, st_size=144, ...}) = 0
fcntl64(3, F_SETFD, FD_CLOEXEC)         = 0
getdents64(3, /* 5 entries */, 4096)    = 160
getdents64(3, /* 0 entries */, 4096)    = 0
close(3)                                = 0
fstat64(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 48), ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
        = 0x40018000
write(1, "ltrace-ls.txt  myfile.txt  strac"..., 41) = 41
munmap(0x40018000, 4096)                = 0
exit_group(0)                           = ?
```

Por ejemplo, si desea seguir los intentos de lectura de un archivo, puede emplear la siguiente expresión:

```
$ strace -e open ls myfile.txt

open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
open("/lib/tls/librt.so.1", O_RDONLY)   = 3
open("/lib/libacl.so.1", O_RDONLY)      = 3
open("/lib/libselinux.so.1", O_RDONLY)  = 3
open("/lib/tls/libc.so.6", O_RDONLY)    = 3
open("/lib/tls/libpthread.so.0", O_RDONLY) = 3
open("/lib/libattr.so.1", O_RDONLY)     = 3
open("/proc/mounts", O_RDONLY)          = 3
[...]
open("/proc/filesystems", O_RDONLY)     = 3
open("/proc/self/attr/current", O_RDONLY) = 4
```

Si lo que necesita es seguir todos los procesos hijo, puede hacerlo mediante la opción `-f`. El comportamiento y formato de salida de strace es ampliamente configurable. Si desea obtener más información al respecto, ejecute el comando `man strace`.

36.18. Llamadas a librerías: ltrace

Las llamadas a librerías por parte de un proceso pueden rastrearse mediante el comando `ltrace`. Su modo de empleo es muy similar al de `strace`. Mediante la opción `-c` puede obtenerse el número y duración de las llamadas a las librerías así como conocer si han sido completadas con éxito:

```
$ strace -c find /usr/share/doc
% time     seconds  usecs/call     calls    errors syscall
------ ----------- ----------- --------- --------- ----------------
 86.27    1.071814          30     35327           write
 10.15    0.126092          38      3297           getdents64
  2.33    0.028931           3     10208           lstat64
  0.55    0.006861           2      3122         1 chdir
  0.39    0.004890           3      1567         2 open
[...]
  0.00    0.000003           3         1           uname
```

```
  0.00    0.000001           1         1           time
------ ----------- ----------- --------- --------- ----------------
100.00    1.242403                 58269         3 total
```

36.19. Librerías necesarias: ldd

Mediante `ldd` es posible visualizar qué librerías ha cargado un ejecutable:

```
$ ldd /bin/ls
linux-gate.so.1 =>  (0xffffe000)
librt.so.1 => /lib/tls/librt.so.1 (0x4002b000)
libacl.so.1 => /lib/libacl.so.1 (0x40033000)
libselinux.so.1 => /lib/libselinux.so.1 (0x40039000)
libc.so.6 => /lib/tls/libc.so.6 (0x40048000)
libpthread.so.0 => /lib/tls/libpthread.so.0 (0x4015d000)
/lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x40000000)
libattr.so.1 => /lib/libattr.so.1 (0x4016d000)
```

Los binarios estáticos no necesitan ninguna librería dinámica:

```
$ ldd /bin/sash
        not a dynamic executable
$ file /bin/sash
/bin/sash: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), \
for GNU/Linux 2.2.5, statically linked, stripped
```

36.20. Información adicional sobre archivos binarios ELF

El programa `readelf` permite leer el contenido de los archivos binarios. Este programa también funciona con archivos ELF construidos para otras arquitecturas de hardware:

```
$ readelf --file-header /bin/ls
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF32
```

```
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Intel 80386
  Version:                           0x1
  Entry point address:               0x8049b40
  Start of program headers:          52 (bytes into file)
  Start of section headers:          76192 (bytes into file)
  Flags:                             0x0
  Size of this header:               52 (bytes)
  Size of program headers:           32 (bytes)
  Number of program headers:         9
  Size of section headers:           40 (bytes)
  Number of section headers:         29
  Section header string table index: 26
```

36.21. Comunicación entre procesos: ipcs

A través del comando `ipcs` es posible obtener un listado de los recursos IPC utilizados:

```
$ ipcs
------ Shared Memory Segments --------
key        shmid      owner      perms      bytes      nattch     status
0x000027d9 5734403    toms       660        64528      2
0x00000000 5767172    toms       666        37044      2
0x00000000 5799941    toms       666        37044      2

------ Semaphore Arrays --------
key        semid      owner      perms      nsems
0x000027d9 0          toms       660        1

------ Message Queues --------
key        msqid      owner      perms      used-bytes   messages
```

36.22. Medida del tiempo con time

El programa de ayuda `time` determina el tiempo consumido por un comando. Este programa está disponible en dos variantes: una versión integrada en la shell (como shell-builtin) y una versión como programa en `/usr/bin/time`.

```
$ time find . > /dev/null

real    0m4.051s
user    0m0.042s
sys     0m0.205s
```

Parte V

Anexo

Fuentes de información y documentación

Existe una gran cantidad de fuentes de información que puede aplicar al sistema SUSE LINUX. Aunque algunas de estas fuentes son específicas para SUSE, otras son de carácter más genérico. Algunas están disponibles en el propio sistema o en el soporte de instalación mientras que otras pueden ser consultadas en Internet.

Documentación de SUSE

Si desea obtener más información, puede consultar la documentación en formato HTML o PDF contenida en los paquetes RPM `suselinux-userguide_es` y `suselinux-adminguide_es`.

Si ha realizado una instalación estándar, los manuales estarán almacenados en el directorio `/usr/share/doc/manual/`. Puede acceder a esta información a través del Centro de Ayuda de SUSE.

The Linux Documentation Project (TLDP)

El proyecto de documentación para Linux (véase `http://www.tldp.org/`) está formado por un equipo de voluntarios que trabajan en la elaboración de diversa documentación acerca de Linux. El TLDP incluye HOWTOs, FAQs, guías y manuales; todo el material publicado está regido por una licencia de libre distribución.

Los HOWTOs consisten en un compendio de instrucciones, detalladas paso a paso y dirigidas al usuario final, administradores de sistemas o programadores. Por

ejemplo, en un HOWTO se describe la configuración de un servidor DHCP y las cuestiones que es necesario tener en cuenta, pero no cómo se instala Linux como tal. Por regla general, esta documentación es de dominio público, de forma que normalmente puede ser aplicada a todas las distribuciones. El paquete `howto` contiene HOWTOs en ASCII. Si prefiere visualizarlos en formato HTML, ha de emplear `howtoenh` en su lugar.

Las FAQs (del inglés, Frequently Asked Questions) son recopilaciones de las preguntas más frecuentes que han sido planteadas por los usuarios (en listas de correo, foros, etc.) así como sus correspondientes respuestas. Por ejemplo, "¿Qué es LDAP?", "¿Qué es RAID?" etc. Generalmente su extensión es breve.

Las guías (guides) tratan los temas de una forma mucho más detallada que los HOWTOs y las FAQs. Por ejemplo, pueden centrarse en la programación del kernel, la administración de redes, etc. Su finalidad es proporcionar al usuario una información en profundidad.

El TLDP incluye también documentos en otros formatos tales como PDF, HTML, PostScript y archivos SGML/XML. Asimismo, parte de la información se encuentra disponible en otros idiomas diferentes del inglés.

Manpages e infopages

Una página del manual o página man (del inglés man page) es un texto de ayuda acerca de un comando, llamada al sistema, formato de archivo o similar. Normalmente, una página del manual se divide en distintas secciones como nombre, sintaxis, descripción, opciones, archivos, etc.

Para mostrar una página del manual, introduzca `man` seguido del nombre del comando, tal como en `man ls`. La expresión anterior muestra el contenido del archivo de ayuda correspondiente al comando `ls`. Puede emplear las teclas del cursor para desplazarse por el documento, mientras que si pulsa la tecla (q) abandonará la utilidad `man`. Si desea imprimir una página del manual (por ejemplo, la correspondiente al comando `ls`), introduzca `man -Tps | lpr`. Para obtener información adicional sobre el comando `man`, utilice la opción `--help` o la página man del propio man (`man man`).

Asimismo, algunos comandos disponen de documentación adicional en formato info, como, por ejemplo, la instrucción `grep`. Para acceder a ella, ha de ejecutar la instrucción `info grep`.

A diferencia de las página del manual, las páginas de información suelen ser bastante extensas y están divididas en distintos "nodos". Un nodo representa una

página que puede ser leída mediante una herramienta del tipo info reader (comparable a un navegador HTML). Para navegar a través de una página de información, se emplean las teclas ⓟ (previous, página anterior) y ⓝ (next, página siguiente). Utilice ⓠ para abandonar el comando `info`. Puede obtener información adicional acerca del manejo de `info` ejecutando `info info`.

Konqueror le permite acceder tanto a las páginas del manual como a las páginas de información mediante la introducción del comando `man:`⟨*expresión*⟩ o `info:`⟨*expresión*⟩ en la línea de URLs.

Estándares y especificaciones

Si desea obtener información acerca de los estándares y especificaciones relacionados con Linux dispone de varias alternativas:

`www.linuxbase.org` Free Standards Group es una organización independiente sin ánimo de lucro cuyo objetivo es ayudar al crecimiento del software abierto y libre. Su misión fundamental es el desarrollo y la promoción de estándares. Bajo la dirección de esta organización se desarrollan estándares muy importantes para Linux tales como LSB (Linux Standard Base).

`http://www.w3.org` El World Wide Web Consortium (W3C) es probablemente una de las instituciones más conocidas dentro del mundo de Internet. La W3C, fundada en octubre de 1994 por Tim Berners-Lee, se centra en la estandarización de tecnologías web. Entre otras tareas, fomenta la aceptación de especificaciones abiertas, de libre distribución e independientes de los fabricantes, como por ejemplo HTML, XHTML y XML. Estos estándares web son desarrollados por grupos de trabajo o *Working Groups* y presentados públicamente como *propuestas de trabajo* (W3C Recommendation (REC)).

`http://www.oasis-open.org` OASIS (Organization for the Advancement of Structured Information Standards) es un consorcio internacional cuya misión es el desarrollo, convergencia y adopción de estándares enfocados a desarrollar el comercio electrónico, transacciones comerciales, logística e interoperabilidad entre distintos fabricantes.

`http://www.ietf.org` La Internet Engineering Task Force (IETF) es una comunidad internacional y abierta formada por investigadores, diseñadores de redes, fabricantes y usuarios. Se centra en el desarrollo de la arquitectura de Internet y que el funcionamiento de ésta se produzca de forma fluida.

Los estándares IETF se publican en formato RFC (Request for Comments). Existen seis tipos de RFCs: proposed standards, draft standards, Internet standards, experimental protocols, informational documents e historic standards. Sólo los tres primeros (propuestos, borrador e Internet) son estándares IETF en sentido estricto (si desea obtener más información, consulte el resumen al respecto en `http://www.ietf.org/rfc/rfc1796.txt`).

`http://www.ieee.org` El Institute of Electrical and Electronics Engineers (IEEE) es una institución que elabora estándares dentro de los ámbitos de las tecnologías de la información, las telecomunicaciones, la medicina y el cuidado de la salud, el servicio de transportes, etc. Los estándares IEEE no son gratuitos.

`http://www.iso.org` El comité ISO (International Organization for Standards) es el mayor desarrollador de estándares del mundo. El ISO dispone de una red de institutos nacionales de estandarización en más de 140 países. Los estándares ISO no son gratuitos.

`http://www.din.de`, **`http://www.din.com`**
El instituto alemán para la normalización (DIN) es una asociación técnico-científica fundada en 1917. Según DIN, es "la autoridad competente para las tareas de normalización dentro de Alemania y representa los intereses de este país ante las organizaciones de estandarización mundiales y europeas".

Esta asociación es una agrupación de fabricantes, usuarios, trabajadores, empresas prestadoras de servicios, científicos u otras personas que tengan interés en la elaboración de documentos de normalización. Estos documentos son de pago y pueden solicitarse a través del sitio web de DIN.

Comprobación del sistema de archivos

Página man de reiserfsck

```
REISERFSCK(8)                                              REISERFSCK(8)

NAME
       reiserfsck - check a Linux Reiserfs file system

SYNOPSIS
       reiserfsck  [  -afprVy ] [ --rebuild-sb | --check | --fix-
       fixable | --rebuild-tree | --clean-attributes  ]  [  -j  |
       --journal device ] [ -z | --adjust-size ] [ -n | --nolog ]
       [ -l | --logfile file ] [ -q | --quiet ] [ -y | --yes ]  [
       -S  |  --scan-whole-partition ] [ --no-journal-available ]
       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
       --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 reis
```

erfs file system" and you are sure that a Reiserfs file system is there.

--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.

--fix-fixable
This option recovers certain kinds of corruption that do not require rebuilding the entire file sys tem tree (--rebuild-tree). Normally you only need this option if the --check option reports "corrup tion that can be fixed with --fix-fixable". This includes: zeroing invalid data-block pointers, cor recting st_size and st_blocks for directories, and deleting invalid directory entries.

--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 , -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-size, -z
This option causes reiserfsck to correct file sizes that are larger than the offset of the last discov ered 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 file, -l file
This option causes reiserfsck to report any corrup tion 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.

   --yes, -y
       This option inhibits reiserfsck from asking you for
       confirmation  after telling you what it is going to
       do, assuming yes. For safety, it does not work with
       the --rebuild-tree option.

   -a, -p These  options are usually passed by fsck -A during
       the automatic checking of those  partitions  listed
       in  /etc/fstab.  These  options cause reiserfsck to
       print some information  about  the  specified  file
       system,  check if error flags in the superblock are
       set and  do  some  light-weight  checks.  If  these
       checks reveal a corruption or the flag indicating a
       (possibly fixable) corruption is found set  in  the
       superblock,  then  reiserfsck  switches to the fix-
       fixable mode. If the flag indicating a  fatal  cor
       ruption  is found set in the superblock, then reis
       erfsck finishes with an error.

   -V     This option prints the  reiserfsprogs  version  and
       exit.

   -r, -f These options are ignored.

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 CODES

reiserfsck uses the following exit codes:

- 0 - No errors.
- 1 - File system errors corrected.
- 4 - File system fatal errors left uncorrected, reiserfsck --rebuild-tree needs to be launched.
- 6 - File system fixable errors left uncorrected, reiserfsck --fix-fixable needs to be launched.
- 8 - Operational error.
- 16 - Usage or syntax error.

AUTHOR

This version of reiserfsck has been written by Vitaly Fertman <vitaly@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, etc.

```
SEE ALSO
       mkreiserfs(8),  reiserfstune(8)  resize_reiserfs(8), debu
       greiserfs(8),

Reiserfsprogs-3.6.9         April 2003              REISERFSCK(8)
```

Página man de e2fsck

```
E2FSCK(8)                                                E2FSCK(8)

NAME
       e2fsck - check a Linux second extended file system

SYNOPSIS
       e2fsck  [ -pacnyrdfvstDFSV ] [ -b superblock ] [ -B block
       size ] [ -l|-L bad_blocks_file ] [ -C fd ] [ -j external-
       journal ] [ -E extended_options ] device

DESCRIPTION
       e2fsck  is used to check a Linux second extended file sys
       tem (ext2fs).  E2fsck also supports ext2 filesystems coun
       taining a journal, which are also sometimes known as ext3
       filesystems, by first applying the journal to the filesys
       tem  before  continuing  with  normal  e2fsck  processing.
       After the journal has been applied, a filesystem will nor
       mally  be  marked  as clean.  Hence, for ext3 filesystems,
       e2fsck will normally run the journal and exit, unless  its
       superblock indicates that further checking is required.

       device  is  the device file where the filesystem is stored
       (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. If this option is specified twice, then the bad block scan will be done using a non-destructive read-write test.

-C fd 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 pro grams which are running e2fsck. If the file descriptor specified is 0, e2fsck will print a com pletion 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).

-D Optimize directories in filesystem. This option causes e2fsck to try to optimize all directories, either by reindexing them if the filesystem sup ports directory indexing, or by sorting and com

```
       pressing  directories  for  smaller directories, or
       for filesystems using traditional  linear  directo
       ries.

-E extended_options
       Set  e2fsck extended options.  Extended options are
       comma separated, and may take an argument using the
       equals  ('=') sign.  The following options are sup
       ported:

            ea_ver=extended_attribute_version
                   Assume  the  format  of  the  extended
                   attribute  blocks  in the filesystem is
                   the specified version number.  The ver
                   sion number may be 1 or 2.  The default
                   extended attribute version format is 2.

-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 block numbers 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.  Note that the block num
       bers  are based on the blocksize of the filesystem.
       Hence, badblocks(8) must be given the blocksize  of
       the  filesystem in order to obtain correct results.
       As a result, it is much simpler and  safer  to  use
       the  -c option to e2fsck, since it will assure that
       the correct parameters are passed to the  badblocks
       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 filesys tem is already in the standard byte-order, e2fsck will take no action.

-S This option will byte-swap the filesystem, regard less 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 follow ing conditions:

```
0    - No errors
1    - File system errors corrected
2    - File system errors corrected, system should
       be rebooted
4    - File system errors left uncorrected
8    - Operational error
16   - Usage or syntax error
32   - E2fsck canceled by user request
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 com
              pletion 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 trou
       ble, try running the debugfs(8) command and send the  out
       put  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 dis
       plays when it is run, so I know which version you are run
       ning.

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 1.34      July 2003                   E2FSCK(8)
```

Manual Page of xfs_check

```
xfs_check(8)                                              xfs_check(8)

NAME
       xfs_check - check XFS filesystem consistency
```

SYNOPSIS

```
xfs_check [ -i ino ] ... [ -b bno ] ... [ -s ] [ -v ] xfs_special

xfs_check -f [ -i ino ] ... [ -b bno ] ... [ -s ] [ -v ] file
```

DESCRIPTION

xfs_check checks whether an XFS filesystem is consistent. It is normally run only when there is reason to believe that the filesystem has a consistency problem. The filesystem to be checked is specified by the xfs_special argument, which should be the disk or volume device for the filesystem. Filesystems stored in files can also be checked, using the -f flag. The filesystem should normally be unmounted or read-only during the execution of xfs_check. Otherwise, spurious problems are reported.

The options to xfs_check are:

-f Specifies that the special device is actually a file (see the mkfs.xfs -d file option). This might happen if an image copy of a filesystem has been made into an ordinary file.

-s Specifies that only serious errors should be reported. Serious errors are those that make it impossible to find major data structures in the filesystem. This option can be used to cut down the amount of output when there is a serious problem, when the output might make it difficult to see what the real problem is.

-v Specifies verbose output; it is impossibly long for a reasonably-sized filesystem. This option is intended for internal use only.

-i ino Specifies verbose behavior for a specific inode. For instance, it can be used to locate all the blocks associated with a given inode.

-b bno Specifies verbose behavior for a specific filesystem block. For instance, it can be used to determine what a specific block is used for. The block number is a "file system block number". Conversion between disk addresses (i.e. addresses reported by xfs_bmap) and file system blocks may be accomplished using xfs_db’s convert command.

Any non-verbose output from xfs_check means that the

filesystem has an inconsistency. The filesystem can be repaired using either xfs_repair(8) to fix the filesystem in place, or by using xfsdump(8) and mkfs.xfs(8) to dump the filesystem, make a new filesystem, then use xfsrestore(8) to restore the data onto the new filesystem. Note that xfsdump may fail on a corrupt filesystem. However, if the filesystem is mountable, xfsdump can be used to try and save important data before repairing the filesystem with xfs_repair. If the filesystem is not mountable though, xfs_repair is the only viable option.

DIAGNOSTICS

Under one circumstance, xfs_check unfortunately might dump core rather than produce useful output. If the filesystem is completely corrupt, a core dump might be produced instead of the message xxx is not a valid filesystem

If the filesystem is very large (has many files) then xfs_check might run out of memory. In this case the message out of memory is printed.

The following is a description of the most likely problems and the associated messages. Most of the diagnostics produced are only meaningful with an understanding of the structure of the filesystem.

agf_freeblks n, counted m in ag a
: The freeblocks count in the allocation group header for allocation group a doesn’t match the number of blocks counted free.

agf_longest n, counted m in ag a
: The longest free extent in the allocation group header for allocation group a doesn’t match the longest free extent found in the allocation group.

agi_count n, counted m in ag a
: The allocated inode count in the allocation group header for allocation group a doesn’t match the number of inodes counted in the allocation group.

agi_freecount n, counted m in ag a
: The free inode count in the allocation group header for allocation group a doesn’t match the number of inodes counted free in the allocation group.

block a/b expected inum 0 got i
: The block number is specified as a pair (allocation group number, block in the allocation group). The block is used multiple times (shared), between multi-

ple inodes. This message usually follows a message of the next type.

block a/b expected type unknown got y
The block is used multiple times (shared).

block a/b type unknown not expected
The block is unaccounted for (not in the freelist and not in use).

link count mismatch for inode nnn (name xxx), nlink m, counted n
The inode has a bad link count (number of references in directories).

rtblock b expected inum 0 got i
The block is used multiple times (shared), between multiple inodes. This message usually follows a message of the next type.

rtblock b expected type unknown got y
The real-time block is used multiple times (shared).

rtblock b type unknown not expected
The real-time block is unaccounted for (not in the freelist and not in use).

sb_fdblocks n, counted m
The number of free data blocks recorded in the superblock doesn't match the number counted free in the filesystem.

sb_frextents n, counted m
The number of free real-time extents recorded in the superblock doesn't match the number counted free in the filesystem.

sb_icount n, counted m
The number of allocated inodes recorded in the superblock doesn't match the number allocated in the filesystem.

sb_ifree n, counted m
The number of free inodes recorded in the superblock doesn't match the number free in the filesystem.

SEE ALSO
mkfs.xfs(8), xfsdump(8), xfsrestore(8), xfs_ncheck(8), xfs_repair(8), xfs(5).

xfs_check(8)

Manual Page of jfs_fsck

```
jfs_fsck(8)       JFS utility - file system check       jfs_fsck(8)

NAME
       jfs_fsck  -  initiate replay of the JFS transaction log, and
       check and repair a JFS formatted device


SYNOPSIS
       jfs_fsck [ -afnpvV ] [ -j journal_device  ]  [  --omit_jour-
       nal_replay ] [ --replay_journal_only ] device


DESCRIPTION
       jfs_fsck  is used to replay the JFS transaction log, check a
       JFS formatted device for errors, and fix any errors found.

       device is the special file name corresponding to the  actual
       device to be checked (e.g. /dev/hdb1).

       jfs_fsck must be run as root.

WARNING
       jfs_fsck should only be used to check an unmounted file sys-
       tem or a file system  that  is  mounted  READ  ONLY.   Using
       jfs_fsck to check a file system mounted other than READ ONLY
       could seriously damage the file system!

OPTIONS
       If no options are selected, the default is -p.

       -a     Autocheck mode - Replay the transaction log.  Do  not
              continue  fsck  processing unless the aggregate state
              is dirty or  the  log  replay  failed.   Functionally
              equivalent  to  -p.   Autocheck mode is typically the
              default mode used when jfs_fsck  is  called  at  boot
              time.

       -f     Replay the transaction log and force checking even if
              the file system appears clean.  Repair  all  problems
              automatically.

       -j journal_device
```

Specify the journal device.

-n Open the file system read only. Do not replay the transaction log. Report errors, but do not repair them.

--omit_journal_replay
Omit the replay of the transaction log. This option should not be used unless as a last resort (i.e. the log has been severely corrupted and replaying it causes further problems).

-p Automatically repair ("preen") the file system. Replay the transaction log. Do not continue fsck processing unless the aggregate state is dirty or the log replay failed. Functionally equivalent to -a.

--replay_journal_only
Only replay the transaction log. Do not continue with a full file system check if the replay fails or if the file system is still dirty even after a journal replay. In general, this option should only be used for debugging purposes as it could leave the file system in an unmountable state. This option cannot be used with -f, -n, or --omit_journal_replay.

-v Verbose messaging - print details and debug statements to stdout.

-V Print version information and exit (regardless of any other chosen options).

EXAMPLES

Check the 3rd partition on the 2nd hard disk, print extended information to stdout, replay the transaction log, force complete jfs_fsck checking, and give permission to repair all errors:

```
jfs_fsck -v -f /dev/hdb3
```

Check the 5th partition on the 1st hard disk, and report, but do not repair, any errors:

```
jfs_fsck -n /dev/hda5
```

EXIT CODE

The exit code returned by jfs_fsck represents one of the following conditions:

```
        0     No errors

        1     File  system  errors corrected and/or transaction log
              replayed successfully

        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

REPORTING BUGS
       If  you  find a bug in JFS or jfs_fsck, please report it via
       the bug tracking system ("Report Bugs" section) of  the  JFS
       project web site:
       http://oss.software.ibm.com/jfs

       Please  send  as  much  pertinent  information  as possible,
       including the complete output of running jfs_fsck  with  the
       -v option on the JFS device.

SEE ALSO
       fsck(8),  jfs_mkfs(8), jfs_fscklog(8), jfs_tune(8), jfs_log-
       dump(8), jfs_debugfs(8)

AUTHORS
       Barry Arndt  (barndt@us.ibm.com)
       William Braswell, Jr.

       jfs_fsck is maintained by IBM.
       See the JFS project web site for more details:
       http://oss.software.ibm.com/jfs

                         October 29, 2002              jfs_fsck(8)
```

Traducción en castellano de 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

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 prohiban 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:

1. Debe procurar que los ficheros modificados incluyan notificaciones destacadas manifestando que los ha cambiado y la fecha de cualquier cambio.

2. 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.

3. 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 licenciatarios 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:

1. 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

2. 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

3. 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 hada 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 licenciatario 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" *("any later version")*, 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/U 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.

```
<Program name and short description>

Copyright (C) <year> <name of author>

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:

```
<Nombre del programa y breve descripción>

Copyright (C)<Año> <Nombre del autor>

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
COMERCIABILIDAD 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 Version 69, Copyright (C) <year> <name of author>
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 versión 69, Copyright (C) <Año> <Nombre del autor>

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.

Glosario

ACL (Lista de Control de Acceso o Access Control List)
Una ampliación del concepto tradicional de permisos para archivos y directorios. Permiten un control más estricto de los permisos de acceso.

Administrador de sistema (system administrator, root user)
Ver root.

ADSL o Línea de Abonado Digital Asimétrica (Asymmetric Digital Subscriber Line)
Sistema de transmisión de alta velocidad que transmite datos a través de la línea telefónica.

AGP (Accelerated Graphics Port)
Puerto rápido para tarjetas gráficas. Está basado en el PCI pero ofrece un ancho de banda mucho mayor que éste. Al contrario que los modelos PCI, las tarjetas gráficas AGP pueden acceder directamente a la memoria RAM y recoger los datos gráficos allí almacenados sin que éstos tengan que pasar antes por el procesador.

Ancho de banda
Máxima capacidad de transmisión de un canal de datos. Se emplea normalmente en referencia a las conexiones de red.

Arranque
Se denomina así todo el proceso de inicio del ordenador, desde el momento de encender la máquina hasta que el sistema se encuentra a disposición del usuario. En el caso de Linux es la iniciación del kernel y el inicio de los servicios del sistema.

ATAPI (Advance Technology Attachment Packet Interface)
Hoy en día más conocida como IDE o bien EIDE. El Advanced procede de la época en que los discos duros eran de 10 MB e increíblemente lentos.

Backup
Denominación en inglés de las copias de seguridad. Siempre se deberían hacer copias de seguridad, especialmente de aquellos datos que consideremos importantes.

BIOS (Basic Input Output System)
Pequeño grupo de programas que se encarga de iniciar los principales componentes de hardware en los primeros segundos del arranque del sistema. La mayoría de las BIOS permiten su configuración mediante la modificación de ciertos parámetros. El código del programa de configuración reside en un chip de sólo lectura (ROM).

Caché
Si se compara con la memoria RAM la caché resulta ser una memoria muy pequeña pero rápida al mismo tiempo. En la caché se guardan por ejemplo archivos que han sido abiertos, de tal forma que si se necesitan poco después no hará falta volverlos a cargar.

Cliente
Un programa o estación de trabajo en una red que conecta y pide servicios a un servidor.

Consola (console, terminal)
Antes sinónimo de terminal. En Linux existen las llamadas *consolas virtuales* que permiten utilizar la pantalla para múltiples sesiones de trabajo paralelas.

Controlador
Programa situado entre el sistema operativo y el hardware que establece la comunicación entre ambas partes.

Cortafuegos (firewall)
Un sistema para filtrar el tráfico de red que protege una red local de accesos externos no autorizados.

CPU (Unidad Central de Proceso o Central Processing Unit)
Ver procesador.

Cuenta
Ver permisos de acceso.

Cuenta de usuario (user account)
Ver cuenta.

Cursor
Pequeño símbolo en forma de raya o cuadrado que indica el lugar exacto en el que se introducirá el siguiente carácter.

Daemon (disk and execution monitor) o demonio
Programa que está de guardia en segundo plano y que actúa en el momento necesario. Los demonios responden por ejemplo a peticiones de HTTP (httpd).

DDC (Direct Display Channel)
Estándar de comunicación entre el monitor y la tarjeta gráfica para transmitir diversos parámetros a la tarjeta tales como el nombre del monitor o la resolución.

Dirección IP
Dirección numérica única (32 bits) compuesta de 4 bloques separados por puntos (por ejemplo 192.168.10.1) y usada para controlar el ordenador en redes TCP/IP.

Directorio (directory)
Los directorios constituyen la estructura del sistema de archivos. El directorio contiene listas de archivos y de subdirectorios.

Directorio de usuario (home directory)
Directorio personal en el sistema de archivos Linux (generalmente `/home/<nombre_usuario>`) perteneciente a un usuario en concreto que es el único que tiene derecho a acceder a él.

Directorio raíz (root directory)
Directorio principal de un sistema de archivos que, a diferencia de los demás, no tiene ningún directorio superior. En UNIX el directorio raíz está representado por el símbolo `/`.

DNS (Domain Name System)
Un protocolo que convierte direcciones basadas en nombres a direcciones IP y viceversa.

E-Mail (electronic mail) o correo electrónico
Sistema para enviar mensajes electrónicos entre los usuarios de una red local o entre sistemas conectados a Internet.

EIDE (Enhanced Integrated Drive Electronics)
Estándar IDE mejorado que permite discos duros con una capacidad de más de 512 MB.

Enlace (link)
Relaciones cruzadas a otros archivos habituales tanto en Internet como en el sistema Linux. En el segundo caso se suele distinguir entre enlaces duros y enlaces simbólicos. Mientras que los enlaces duros apuntan a una posición en el sistema de archivos, la variante simbólica sólo apunta al nombre correspondiente.

Entorno (environment)
La shell proporciona normalmente un entorno que permite al usuario realizar definiciones temporales. Estas definiciones son por ejemplo las rutas hacia determinados programas, el nombre de usuario, la ruta actual, el aspecto del prompt, etc. Estos datos se almacenan en variables de entorno. Normalmente son los archivos de configuración de la shell los que se ocupan de definir estas variables de entorno.

Ethernet
Hardware de amplia difusión para redes de pequeñas dimensiones con estructura de bus.

EXT2 (Second Extended File System)
Sistema de archivos estándar de Linux.

FAQ (Preguntas de Uso Frecuente o Frequently Asked Questions)
Acrónimo de uso muy extendido utilizado para designar un documento que contiene respuestas a preguntas que se realizan con frecuencia sobre un tema concreto.

FTP (Protocolo de Transferencia de archivos o File Transfer Protocol)
Protocolo basado en TCP/IP utilizado para la transferencia de archivos.

Gestor de ventanas (window manager)
Capa basada en el sistema X Window que se ocupa principalmente de la representación del escritorio. Existen numerosos gestores de ventanas como por ejemplo KDE, uno de los más conocidos.

GNOME (GNU Network Object Model Environment)
Entorno gráfico de escritorio de Linux de cómoda utilización al igual que KDE.

GNU (GNU is Not Unix)
GNU es un proyecto de la Free Software Foundation (FSF). El objetivo del Proyecto GNU es la creación de un sistema operativo libre, compatible con el sistema operativo Unix. Libre no hace referencia tanto a *libre de costes* sino más bien a la libertad en cuanto al derecho de acceso, modificación y utilización de los programas. Para que el código fuente (source) se mantenga libre, cualquier modificación en él también debe serlo. En el clásico Manifiesto GNU (`http://www.gnu.org/gnu/manifesto.html`) se explica la forma en que se asegura la libertad de GNU. Todo ello está respaldado jurídicamente por la licencia pública GPL (General Public License) que se encuentra en `http://www.gnu.org/copyleft/gpl.html` y LGPL (Lesser General Public License) disponible en `http://www.gnu.org/copyleft/lgpl.html`. El kernel de Linux, con licencia GPL, se beneficia de este proyecto (especialmente por las herramientas) pero no es equivalente al proyecto GNU.

GPL (GNU GENERAL PUBLIC LICENSE)
Ver GNU.

Hostname
Nombre que recibe un ordenador en Linux y bajo el cual casi siempre se le puede hallar en la red.

HTML (Hypertext Markup Language)
Principal lenguaje utilizado en la red World Wide Web para mostrar contenidos. Los comandos que componen este lenguaje definen el aspecto con el que un navegador muestra un documento en pantalla.

HTTP (Protocolo de Transferencia de Hipertexto Hypertext Transfer Protocol)
: Protocolo de comunicación entre navegadores y servidores de Internet que sirve para transmitir páginas HTML en la red World Wide Web.

IDE (Integrated Drive Electronics)
: Un estándar de conexión de discos duros.

Internet
: Red mundial de ordenadores basada en TCP/IP.

IRQ (Interrupt Request)
: Solicitud (asíncrona) dirigida desde un componente de hardware o desde un programa al sistema operativo requiriendo un tiempo de CPU. La mayoría de las IRQs están controladas por el sistema operativo.

KDE (K Desktop Environment)
: Interfaz gráfica de Linux de cómoda utilización al igual que GNOME.

Kernel
: Núcleo del sistema operativo Linux donde se sitúa la mayor parte de los programas y controladores. Gestiona la memoria, sistemas de archivos, procesos y la comunicación a través de la red.

LAN (Red de Área Local local area network)
: Red de área local, normalmente de tamaño reducido.

LILO (cargador de Linux o Linux Loader)
: Pequeño programa que se instala en el sector de arranque (bootsector) y que puede arrancar tanto Linux como otros sistemas operativos.

Línea de comandos (prompt)
: Caracteriza la posición de un texto ubicado en la shell donde los comandos del sistema operativo pueden ser introducidos.

Linux
: Núcleo del sistema operativo de tipo UNIX distribuido libremente bajo licencia GPL (GNU), denominado así por su creador Linus Torvalds (Linus' uniX). Si bien en el sentido estricto este término designa sólo al kernel, por *Linux* se entiende generalmente todo el sistema, aplicaciones incluidas.

Login
Registro que realiza un usuario cada vez que solicita permiso para acceder a un sistema o red.

Logout
Acción que se realiza al salir del sistema.

Manual pages
Tradicionalmente en el sistema Unix la documentación se encuentra en forma de manual pages o manpages (páginas man) que se pueden visualizar con el comando `man`.

Marcador (bookmark)
Lista, generalmente personal, de enlaces a páginas web interesantes disponible directamente en el navegador.

MBR (Registro de Arranque Maestro o Master Boot Record)
Primer sector físico de un disco duro. Su contenido se carga en la memoria RAM y se ejecuta por la BIOS al arrancar el sistema. Este código carga entonces el sistema operativo desde una partición del disco duro o desde un gestor de arranque, como por ejemplo LILO o GRUB.

MD5
Algoritmo para generar sumas de control. Estas sumas de control son generadas de tal forma que sea virtualmente imposible crear un archivo que disponga del mismo valor MD5 que un archivo de contenido diferente.

Memoria RAM (Memoria de Acceso Aleatorio o Ramdom Access Memory)
Memoria física del ordenador de capacidad limitada y de rápido acceso.

Montar
Incorporación de un sistema de archivos en el árbol de directorios del sistema.

MP3
Método (con muchas pérdidas) para comprimir archivos de audio que permite reducir el tamaño del archivo a una décima parte del tamaño original.

Multitarea (multitasking)
Capacidad de ciertos sistemas operativos de ejecutar varias aplicaciones a la vez.

Multiusuario
Posibilidad de que varios usuarios trabajen a la vez en un mismo sistema.

Navegador
Programa de búsqueda y visualización de contenidos. Hoy en día utilizado principalmente en programas que representan contenidos de la World Wide Web de forma gráfica.

NFS (Network File System)
Protocolo de acceso a sistemas de archivos de ordenadores conectados en red.

NIS (Network Information Service)
Sistema de gestión central de datos administrativos en redes. Principalmente, NIS permite mantener sincronizados los nombres de usuario y las contraseñas dentro de la red.

Partición
Sección de un disco duro que contiene un sistema de archivos o espacio de intercambio.

Permisos de acceso (account)
Unidad compuesta por el nombre de usuario (login name) y la contraseña (password). Una cuenta se corresponde con un ID de usuario (UID). Los permisos de acceso suelen ser establecidos por el administrador de sistema. Este establece también a qué grupo de usuarios pertenece un usuario nuevo y qué tipo de derechos se le adjudican en el sistema.

Plug and Play
Tecnología para la detección automática de componentes de hardware y protocolo de configuración.

Procesador
El procesador es el cerebro del ordenador que procesa y ejecuta los comandos del usuario o los programas en lenguaje máquina. Tiene el control del sistema y se encarga del cálculo propiamente dicho.

Proceso (process)
Un programa en ejecución. A menudo se utiliza este término como sinónimo de tarea.

Prompt
El prompt o la petición de entrada en una shell marca el sitio en el que se pueden introducir comandos dirigidos al sistema operativo.

Protocolo (protocol)
Estándar específico definido que regula la comunicación a nivel de hardware, software y red. Existen varios de estos estándares de entre los que HTTP y FTP son de los más populares.

Proxy
Normalmente se define como un ordenador que sirve de almacenamiento intermedio para los datos transferidos desde Internet. Si el mismo documento es solicitado más de una vez, la segunda petición será servida mucho más rápidamente. Los ordenadores que desee aprovechar esta ventaja han de ser configurados para realizar sus peticiones a través del proxy.

RAM (Random Access Memory)
Ver memoria RAM.

RDSI
Red digital de servicios integrados; estándar para la transmisión digital de datos a través de la red telefónica.

Red (net, network)
Unión de varios ordenadores formada en la mayoría de los casos por un servidor y unos clientes que permite la transferencia de datos entre ellos. El ordenador que envía una solicitud a la red se denomina normalmente como cliente mientras que al ordenador que le responde se le suele designar servidor.

ReiserFS
Sistema de archivos que registra los cambios efectuados en él en un diario o journal. Esto hace que el sistema de archivos pueda restablecerse muy rápidamente y repararse las potenciales inconsistencias. Tales inconsistencias pueden producirse cuando un sistema de archivos no ha sido montado antes de salir del sistema operativo, por ejemplo, en el caso de un fallo de alimentación.

Root (system administrator, root user)
Persona que se encarga de la configuración y el mantenimiento de un sistema complejo de ordenadores o de una red. Este administrador de sistema, que suele ser una sola persona, tiene acceso a todas las posibilidades de configuración de un sistema (derechos root). Este tipo de cuenta no debe utilizarse para el trabajo del día a día.

Ruta (path)
Localización exacta de un archivo en un sistema de archivos. En Unix, los distintos niveles de directorios se separan mediante el símbolo de la barra `/`.

SCSI (Small Computer Systems Interface)
Estándar para la conexión de discos duros y otros dispositivos tales como unidades de cinta y escáneres.

Servidor
Ordenador de gran rendimiento que proporciona datos y servicios a otros ordenadores (clientes) conectados a través de una red. Algunos de estos servicios son HTTP, DNS y FTP servidores.

Shell
Programa interactivo que permite la ejecución de comandos. bash, zsh y tcsh son algunos ejemplos de shell.

Sistema de archivos (file system)
Sistema para ordenar los archivos. Existen muchos sistemas de archivos que difieren en función de sus prestaciones.

Sistema operativo (operating system)
Ver kernel.

Sistema X Window
El sistema X Window en un sistema de ventanas basado en red que funciona en una gran variedad de ordenadores. Ofrece funciones primitivas como el trazado de líneas o rectángulos. Representa la capa intermedia entre el hardware y el gestor de ventanas.

SMTP (Simple Mail Transfer Protocol)
Protocolo para la transmisión de correo electrónico.

Software libre
Ver GNU.

SSL (Secure Socket Layer)
Sistema para codificar transmisiones de datos HTTP.

Superusuario (super user)
Ver root.

Tarea
Ver proceso.

TCP/IP
Protocolo de comunicación de Internet empleado también en la mayoría de las redes locales.

Telnet
Telnet es el protocolo y comando usado para comunicarse con otros ordenadores que se convierten de este modo en anfitriones (hosts). En el caso de accesos remotos, se reemplaza normalmente por SSH, debido a que éste proporciona una conexión codificada.

Terminal (terminal)
Antes era el nombre que recibía una combinación de monitor y teclado conectada a un sistema central sin capacidad propia de cálculo, también denominado unidad de visualización o estación de datos . En el caso de estaciones de trabajo, el término también se usa para hablar de programas que emulan una terminal real tales como xterm.

Tux
Nombre del pingüino mascota de Linux (véase `http://www.sjbaker.org/tux/`).

UNIX
UNIX es una marca registrada así como un tipo de sistema operativo.

URL (Uniform Resource Locator)
Dirección de Internet que contiene el protocolo (como, por ejemplo, `http://`), el nombre del ordenador y dominio (`www.suse.de`) y un documento (por ejemplo, `/us/company/index.html`). La URL completa del ejemplo sería `http://www.suse.de/us/company/index.html`

Variable de entorno (environment variable)
Lugar en el entorno de la shell. Cada variable de entorno posee un nombre (generalmente en mayúsculas) y un valor, por ejemplo la ruta de un archivo (pathname).

VESA (Video Electronics Standard Association)
Consorcio industrial que define, entre otros, importantes estándares para vídeo.

Wildcard
Símbolo que representa un carácter (símbolo: ?) o varios caracteres (símbolo: *) desconocidos. Es utilizado principalmente en comandos (generalmente de búsqueda).

Windowmanager
Ver gestor de ventanas.

WWW (World Wide Web)
Parte gráfica de Internet basada en el protocolo HTTP y que puede ser explorada mediante los llamados navegadores de red.

X11
Versión 11 del sistema X Window.

YaST (Yet another Setup Tool)
El asistente del sistema de SUSE LINUX.

YP (Páginas Amarillas yellow pages)
Ver NIS.

Índice alfabético

B

C

D

E

F

G

H

I

J

K

L

M

R

S

T

U

V

W

X

Y

Z