SUSE LINUX

Manuale di amministrazione

Edizione 3 2005

Vi preghiamo di rivolgere eventuali comunicazioni e commenti all'indirizzo sottostante: `mailto:documentation@suse.de`.

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

Traduttori: Gaetano Lazzara

Redazione: Jörg Arndt, Karl Eichwalder, Antje Faber, Berthold Gunreben, Roland Haidl, Jana Jaeger, Edith Parzefall, Ines Pozo, Thomas Rölz, Thomas Schraitle

Formato: Manuela Piotrowski, Thomas Schraitle

Composizione:DocBook-XML, LaTeX

Questo manuale è stato stampato su carta sbiancata senza cloro.

Benvenuti

Congratulazioni per il vostro nuovo sistema operativo Linux, e grazie per aver scelto SUSE LINUX 9.3. Con l'acquisto della presente versione di SUSE LINUX avete anche acquisito il diritto di usufruire del servizio di supporto all'installazione, per via telefonica o e-mail, come descritto all'indirizzo `http://www.novell.com/products/linuxprofessional/support/conditions.html`. Indicando il codice riportato sulla custodia dei CD sul portale di SUSE LINUX (`http://portal.suse.com`) vi registrate per poter usufruire del servizio di supporto.

Affinché il vostro sistema sia sempre aggiornato e sicuro, consigliamo di eseguire ad intervalli regolari un aggiornamento tramite il comodo YaST Online Update. Un ulteriore servizio a vostra disposizione è la e-newsletter gratuita che vi informerà regolarmente sulle questioni inerenti alla sicurezza del sistema e che inoltre vi fornirà consigli e trucchetti in tema di SUSE LINUX. Potete registrarvi, indicando semplicemente il vostro indirizzo di posta elettronica, sotto `http://www.novell.com/company/subscribe/`.

Il *Manuale di amministrazione* di SUSE LINUX fa luce sulle nozioni fondamentali riguardanti il funzionamento del vostro sistema SUSE LINUX. Il presente manuale vi introduce nell'amministrazione di un sistema Linux, cominciando dalle basi, e cioé file system, kernel, processo di boot fino ad arrivare a trattare la configurazione di un server web Apache. Il *Manuale di amministrazione* di SUSE LINUX è strutturato nel modo seguente:

Installazione Descrizione dell'intero processo di installazione e configurazione del sistema tramite YaST con dettagli che trattano varianti di installazione particolari, LVM, RAID, aggiornamento e ripristino del sistema.

Sistema Caratteristiche proprie di SUSE LINUX, illustrazione dettagliata del kernel, varianti di boot e processo di inizializzazione, configurazione di un boot loader e del sistema X Window nonché del processo di stampa e del computing mobile sotto Linux.

Servizi Integrazione in reti eterogenee, configurazione di un server web Apache, sincronizzazione di file e impostazioni riguardanti la sicurezza.

Amministrazione ACL per file system e importanti strumenti per il monitoraggio del sistema.

Appendice Principali fonti di informazioni su Linux.

La versione digitale dei manuali di SUSE LINUX è reperibile nella directory `/usr/share/doc/manual/`.

Novità nel manuale di amministrazione

Ecco le novità rispetto alla versione precedente del presente manuale (SUSE LINUX 9.2):

- Sono state rimaneggiate le sezioni su LVM ed il partizionamento. Si veda anche la sezione 3.6 a pagina 98 e sezione 2.7.5 a pagina 73
- Il capitolo 8 a pagina 177 è stato rivisitato ed aggiunta una illustrazione del relativo modulo di YaST. Inoltre contiene una nuova sezione sull'utilizzo delle wild card (si veda la sezione Le wild card e la selezione del kernel di boot a pagina 186).
- Nel capitolo sui filesystem troverete una nuova sezione che tratta il filesystem Reiser4. Si veda la sezione 20.2.5 a pagina 378.
- I capitoli che trattano gli aspetti inerenti ad una rete sono stati rivisitati e ristrutturati. Si veda la capitolo 22 a pagina 397 e capitoli successivi.
- Il capitolo che tratta del SuSEfirewall2 è stato aggiornato, ed è stata aggiunta una descrizione del nuovo modulo di YaST; si veda anche la sezione Configurazione con YaST a pagina 609.
- Sotto capitolo 36 a pagina 647 vengono illustrati tutta una serie di nuovi programmi.
- Il glossario è stato aggiornato, si veda anche il Glossary V a pagina 701.

Convenzione tipografica

Nel presente manuale si utilizzano le seguenti convenzioni tipografiche:

- `/etc/passwd`: un nome di un file o directory.
- ⟨*Segnaposto*⟩: la sequenza di caratteri di ⟨*Segnaposto*⟩ va sostituita col valore effettivo.
- `PATH`: variabile di ambiente di nome PATH
- `ls`: un comando.
- `--help`: opzioni e parametri.
- `user`: un utente.
- Alt: tasto da premere.
- 'File': voci di menu, tasti.
- Process killed: messaggi del sistema.
- man man(1): rinvio ad una pagina di manuale
- ► **x86, AMD64**
  Questo paragrafo vale solo per le architetture indicate. Le frecce segnano l'inizio e la fine del testo. ◄

Riconoscimenti

È l'impegno volontario degli sviluppatori di Linux, che collaborano a livello mondiale, a promuovere lo sviluppo di Linux. Un grazie da parte nostra per i loro sforzi — senza di loro non ci sarebbe questa distribuzione. Vorremmo ringraziare inoltre Frank Zappa e Pawar. E chiaramente vorremmo ringraziare in modo particolare Linus Torvalds.

Have a lot of fun!

Il vostro Team SUSE

Indice

Parte I

Installazione

Installazione con YaST

Nel presente capitolo vi illustreremo l'installazione del vostro sistema SUSE LINUX attraverso l'assistente di sistema di YaST. Faremo luce su come preparare il processo di installazione e approfondiremo le singole tappe del processo di configurazione per aiutarvi a prendere le decisioni giuste nella varie fasi del processo di configurazione.

1.1 Avvio del sistema ai fini dell'installazione

Inserite il dispositivo di installazione di SUSE LINUX nell'apposito lettore e riavviate il sistema; verrà caricato il programma di installazione e si avvierà il processo di installazione.

1.1.1 Opzioni di boot

Oltre all'avvio dal CD o DVD potete caricare il sistema anche in vario modo. Queste possibilità si rivelano utili soprattutto quando si è alle prese con delle difficoltà nell'avvio da CD o DVD. Le opzioni sono descritte nella tabella 1.1 in questa pagina.

Tabella 1.1: *Opzioni di boot*

Opzioni di boot	**Utilizzo**
CD-Rom	Si tratta della possibilità più semplice di eseguire il boot. Il sistema deve disporre di un lettore di CD-Rom locale supportato da Linux.
Floppy	Sul primo CD, nella directory `/boot/` trovate le immagini necessarie per creare un dischetto di boot. Vi è anche un `README` nella stessa directory.
PXE o BOOTP	Questa funzionalità deve essere supportata dal BIOS o firmware del sistema in questione e sulla rete deve esservi un server di boot. Anche un altro sistema SUSE LINUX può fungere da server di boot.
Disco rigido	SUSE LINUX può essere caricato anche dal disco rigido. Copiate il kernel (`linux`) ed il sistema di installazione (`initrd`) dalla directory `/boot/loader` del primo CD sul disco rigido, e aggiungete la relativa registrazione al boot loader.

1.1.2 Eventuali difficoltà all'avvio del sistema

Nel caso in cui il vostro harware sia piuttosto datato oppure non viene supportato, potrebbero verificarsi dei problemi in fase di avvio. Probabilmente il vostro lettore di CD-ROM non riesce a leggere la boot image sul primo CD. In questi casi utilizzate il CD 2 per avviare il sistema. Questo CD contiene una boot image tradizionale di 2.88 Mbyte che può essere letta anche da lettori non proprio recenti. In questo caso sussiste comunque la possibilità di eseguire il boot da CD e di realizzare l'installazione tramite la rete.

La sequenza di boot non è stata impostata correttamente nel BIOS (Basic Input Output System). Per maggiori informazioni in tema di modifiche delle impostazioni del BIOS, consultate la documentazione della vostra scheda madre o le sezioni seguenti.

Il BIOS avvia le funzionalità di base del sistema. I produttori di scheda madre forniscono un BIOS specifico per il proprio hardware. Si può accedere al setup del BIOS solo in un momento ben preciso, infatti, all'avvio del sistema viene analizzato l'hardware come la RAM, (processo le cui fasi potete seguire sullo schermo) mentre contemporaneamente, in basso, vi viene comunicato tramite quale tasto è possibile accedere al setup del BIOS. Di solito si tratta dei tasti (Canc), (F1) o (Esc). Premete il relativo tasto per avviare il BIOS-Setup.

Importante

Mappatura dei tasti nel BIOS

Spesso il BIOS presenta la mappatura dei tasti di una tastiera americana: i tasti (Y) e (Z) potrebbero risultare invertiti.

Importante

Modificate la sequenza di caricamento nel modo seguente: nel caso di un BIOS AWARD cercate la voce 'BIOS FEATURES SETUP'; altri produttori usano indicazione del tipo 'ADVANCED CMOS SETUP' o simili. Fate la vostra selezione e confermate con (Invio).

La sequenza di caricamento si può impostare alla voce 'BOOT SEQUENCE'. Il valore preimpostato è spesso 'C, A' o 'A, C'. Nel primo caso, il sistema al suo avvio cerca il sistema operativo prima sul disco rigido (C) e, poi, sul lettore di dischetti (A). Premete (Pag Su) o (Pag Giù) fino ad avere la sequenza 'A,CDROM,C'.

Uscite dal setup premendo (Esc). Per salvare le vostre modifiche, selezionate 'SAVE & EXIT SETUP' o premete (F10). Confermate le vostre impostazioni con (Y).

Se disponete di un lettore CD-Rom tipo SCSI, nel caso di un Adaptec Hostadapter ad esempio dovete invocarne il BIOS tramite Ctrl-A. Dopo aver selezionato 'Disk Utilities' il sistema visualizza l'hardware connesso: annotatevi l'ID di SCSI del vostro CD-Rom. Uscite dal menu con Esc per aprire in seguito 'Configure Adapter Settings'. Alla voce 'Additional Options', troverete 'Boot Device Options'. Selezionate questo menu e premete Invio. Digitate ora l'ID del lettore CD-Rom che vi siete annotati e premete di nuovo su Invio. Per tornare alla schermata di partenza del BIOS di SCSI, premete due volte Esc , uscite dopo aver confermato con 'Yes' per eseguire nuovamente il boot del sistema.

1.2 Schermata d'avvio

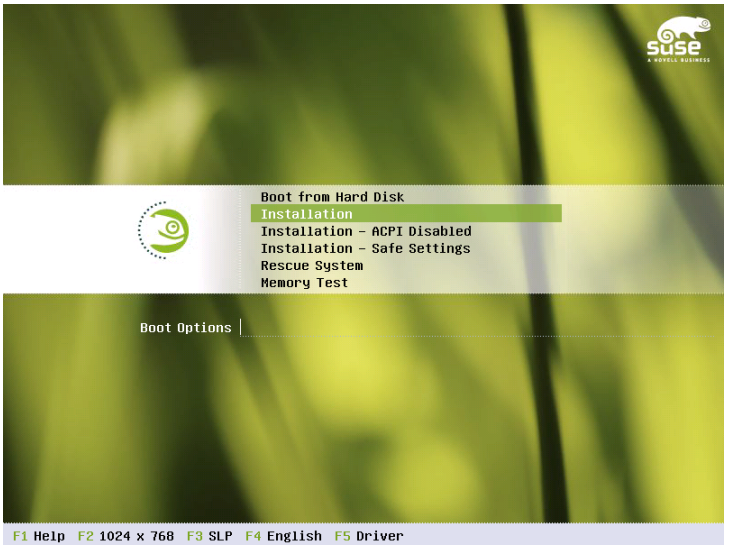

Figura 1.1: *La schermata d'avvio*

La schermata di avvio presenta diverse opzioni per l'ulteriore decorso del processo di installazione. La prima è 'Boot from Harddisk', che carica il sistema già installato. Questa opzione è evidenziata, perché il CD spesso viene lasciato nell'apposito lettore anche ad installazione avvenuta per aggiungere ed installare

del software. Per procedere con l'installazione del sistema, selezionate con i tasti freccia una delle opzioni di installazione. Le opzioni a vostra disposizione sono:

Installazione Il comune modo di installazione. Vengono abilitate tutte le funzioni hardware moderne.

Installazione - ACPI disabled Se la normale installazione fallisce, la causa probabilmente è da ricercare nel fatto che l'hardware non supporta l'ACPI (Advanced Configuration and Power Interface). Con questa opzione avviate quindi un'installazione senza supporto ACPI.

Installazione — Safe Settings Viene disabilita la funzione DMA (per il lettore del CD-Rom) e la funzionalità per il risparmio energetico (power management). Gli esperti possono inserire o modificare qui i parametri del kernel servendosi della riga di comando.

Usate i tasti funzione riportati nella parte bassa dello schermo per intervenire sulle impostazioni durante l'installazione.

(F1) Vi offre assistenza relativamente all'elemento selezionato nella schermata di avvio.

(F2) Seleziona la modalità grafica per l'installazione. Se durante l'installazione in modalità grafica dovessero sorgere delle difficoltà, avete la possibilità di selezionare la modalità testuale.

(F3) Seleziona la fonte di installazione: di solito l'installazione viene eseguita da un supporto di installazione inserito nell'apposito lettore. Comunque avete la possibilità di selezionare altre origini di installazione, ad esempio potete eseguire l'installazione tramite FTP o NFS. Se l'installazione avviene via rete tramite un server SLP (Service Location Protocol) potete selezionare una delle origini disponibili usando questa opzione. Per maggiori informazioni su *SLP* rimandiamo al capitolo 23 a pagina 441.

(F4) Imposta la lingua della schermata di avvio.

(F5) Tramite questo tasto indicate al sistema che disponete di un dischetto di aggiornamento dei driver per SUSE LINUX. Durante l'installazione vi verrà chiesto di inserire il dischetto con gli aggiornamenti.

Dopo un paio di secondi, SUSE LINUX carica un sistema Linux minimale che gestirà le fasi successive del processo di installazione; se avete selezionato 'Native' o 'Verbose' vedrete una serie di comunicazioni ed indicazioni sui diritti d'autore del programma. Infine viene caricato il programma di installazione YaST, e dopo pochi secondi vedrete l'interfaccia grafica del programma di installazione.

A questo punto inizia l'installazione vera e propria di SUSE LINUX. Tutte le schermate di YaST sono strutturate allo stesso modo. Tutte le aree d'inserimento, gli elenchi ed i pulsanti delle schermate di YaST possono essere manovrate con il mouse. Se il cursore del mouse non si muove, vuol dire che il vostro mouse non è stato rilevato automaticamente. In questo caso, usate per il momento la tastiera. L'uso della tastiera in YaST è simile a quanto descritto nella sezione 2.9.1 a pagina 82.

1.3 Selezione della lingua

SUSE LINUX e YaST si adattano alla lingua da voi scelta. Questa impostazione viene applicata anche alla mappatura della tastiera. Inoltre, YaST imposta anche il fuso orario più probabile in base alla lingua da voi selezionata. Queste impostazioni si lasciano modificare anche dopo quando selezionerete una lingua secondaria da installare sul vostro sistema. Se il mouse continua a non funzionare, usate i tasti a freccia per selezionare la lingua desiderata e premete il tasto (Tab), finché non arrivate al pulsante 'Accetta'. Con (Invio) la selezione diviene effettiva.

1.4 Tipo di installazione

Decidete qui se eseguire una 'Nuova installazione' o un 'Aggiornamento del sistema esistente'. Va da sé che l'ultima opzione funziona solo se avete già installato una versione di SUSE LINUX. In questo caso, potete anche caricare il sistema con 'Avviare sistema installato'. Se il sistema già installato dovesse non avviarsi più (magari perché sono state cancellate delle importanti configurazioni di sistema), selezionate 'Ripara sistema installato' per tentare di rendere nuovamente avviabile il sistema. Se finora non è stato installato alcun sistema SUSE LINUX chiaramente non potrete eseguire una reinstallazione (si veda la figura 1.3 a pagina 10).

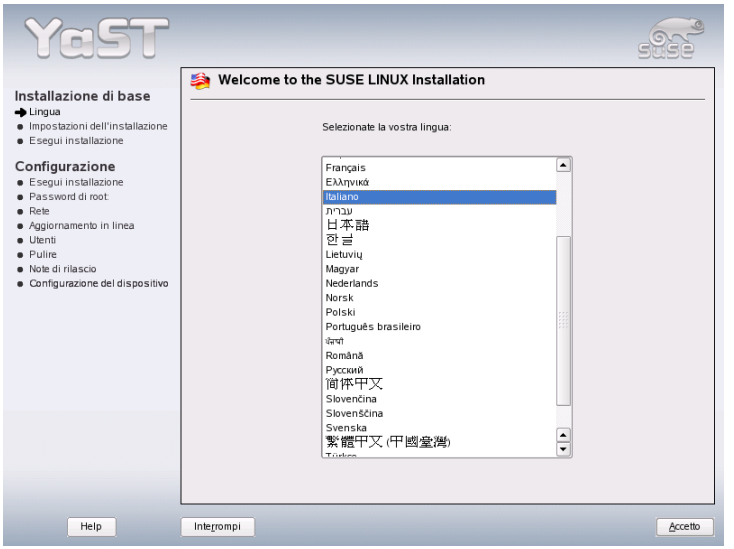

Figura 1.2: *La scelta della lingua*

In questo paragrafo, descriveremo il decorso di una installazione eseguita per la prima volta. Per maggiori dettagli sull'aggiornamento del sistema, consultate la sezione 2.2.5 a pagina 51. Una descrizione delle possibilità riguardanti il modulo di riparazione è reperibile nel capitolo 5 a pagina 143.

1.5 Proposta di installazione

Dopo la rilevazione dell'hardware, si apre una finestra (si veda la figura 1.4 a pagina 11) con delle informazioni sull'hardware rilevato dal sistema e una proposta di installazione e partizionamento. Ci soffermeremo ora sulle singole impostazioni dell'installazione. Se desiderate cambiare qualcosa, fate clic sull'opzione che desiderate modificare.

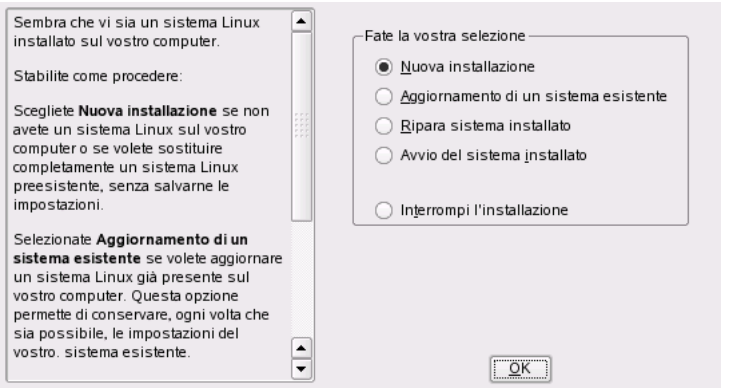

Figura 1.3: *Scelta del tipo di installazione*

1.5.1 Tipo di installazione

Serve per cambiare il tipo di installazione scelto in precedenza. Le opzioni sono le stesse già descritte nella sezione 1.4 a pagina 8.

1.5.2 Mappatura della tastiera

Determinate la mappatura della vostra tastiera, che, normalmente, corrisponde alla lingua precedentemente scelta. Digitate in seguito (é) o (è) per verificare la rappresentazione corretta degli accenti. Con 'Prossimo' tornate alla finestra delle proposte.

1.5.3 Mouse

Se YaST non riconosce automaticamente il mouse, usate per il momento il tasto (Tab) fino a giungere all'opzione 'Mouse'. Tramite la barra spaziatrice ottenete la finestra riprodotta nella figura 1.5 a pagina 12 dove potrete selezionare il tipo di mouse.

Per selezionare il tipo di mouse, usate i tasti (↑) e (↓). La documentazione del vostro mouse dovrebbe fornire indicazioni per effettuare una scelta corretta. Selezionato un mouse potete eseguire un test con la combinazione (Alt)-(T) senza

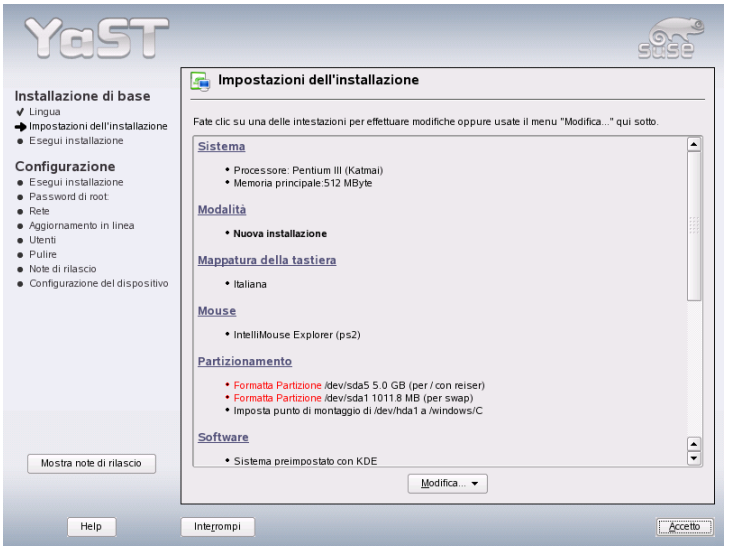

Figura 1.4: *La finestra di dialogo di proposta*

doverlo selezionare definitivamente (se il mouse non reagisce adeguatamente, scegliete e testate un altro tipo). Con Tab e Invio selezionate un mouse in modo permanente.

1.5.4 Partizionamento

Nella maggior parte dei casi, la proposta di partizionamento di YaST può essere applicata senza dover apportare delle modifiche. Nessuno vi impedisce, naturalmente, di ricorrere ad uno schema di partizionamento vostro. Ecco come fare:

Tipi di partizioni

Ogni disco rigido contiene una tabella di partizionamento con quattro voci: ogni voce della tabella può essere una partizione primaria o secondaria, oppure una partizione estesa, che però non può essere più di *una*.

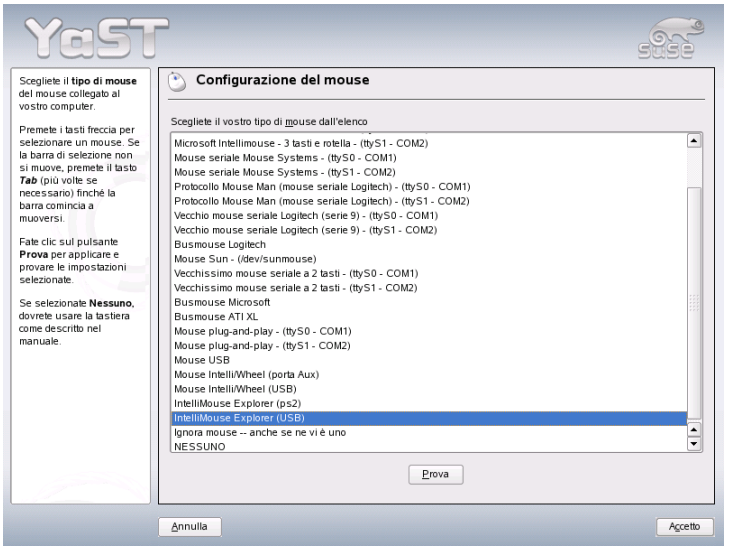

Figura 1.5: *Selezionare il tipo di mouse*

Le partizioni primarie consistono semplicemente in un settore ininterrotto di cilindri (i settori fisici di un disco) attribuiti ad un sistema operativo. Un disco rigido può contenere al massimo quattro partizioni primarie. La tabella delle partizioni offre infatti solo spazio per quattro partizioni. È a questo punto che entrano in gioco le partizioni estese: anche la partizione estesa è una sequenza ininterrotta di cilindri del disco. Ma questa partizione può contenere a sua volta altre cosiddette *partizioni logiche*, che non occupano alcun posto nella tabella delle partizioni. Ogni partizione estesa, è per così dire un contenitore di partizioni logiche.

Se vi occorrono più di quattro partizioni, dovrete solo partizionare il vostro disco in modo tale che almeno la quarta partizione sia una partizione estesa e riceva l'intera sezione dei cilindri ancora disponibili. In questa partizione, potrete poi configurare fino a 15 partizioni logiche per dischi SCSI e 63 partizioni per dischi (E)IDE. Per l'installazione di Linux vanno bene entrambi i tipi di partizione (primaria e logica).

Suggerimento

Dischi rigidi con etichetta GPT

In architetture che usano l'etichetta (ingl. label) GPT, il numero di partizioni primarie non è limitato. In questo caso non sono previste delle partizioni logiche.

Suggerimento

Indicazioni riguardanti la memoria

Se partizionate il vostro disco con YaST, non avete bisogno di preoccuparvi del fabbisogno di memoria e della suddivisione del disco rigido. Se invece partizionate manualmente, tenete presente che ogni tipo di sistema presenta delle esigenze diverse in termini di memoria:

Sistema minimale: 500 Mbyte Questo sistema non ha un'interfaccia grafica (X11), il che significa che potete lavorare solo dalla console. Inoltre, il software da poter installare si limita a quello che non richiede una interfaccia grafica per funzionare.

Sistema minimale con interfaccia grafica: 700 Mbyte
Su questo sistema, potete installare X11 con alcune applicazioni.

Sistema standard 2,5 Gbyte Potrete installare ambienti desktop moderni, come KDE o GNOME) e applicazioni del tipo OpenOffice, Netscape o Mozilla.

Lo spazio da destinare alle diverse partizioni è strettamente legato all'utilizzo a cui è destinato il sistema e allo spazio disponibile. Di seguito sono riportate alcune linee guida che riguardano il partizionamento in funzione dello spazio libero che avete a disposizione:

Fino a ca. 4 Gbyte: Una partizione swap e una partizione root (`/`). La partizione root includerà anche quelle directory per le quali, nel caso di dischi rigidi di notevoli dimensioni, sono spesso previste delle proprie partizione.

Da 4 Gbyte in su: Una partizione swap, una partizione root (1 Gbyte) ed eventualmente rispettivamente una partizione per `/usr` (4 Gbyte o più), `/opt` (4 Gbyte o più) e `/var` (1 Gbyte). Lo spazio libero rimanente può essere dedicato alla directory `/home`.

A seconda dell'hardware del computer può essere necessario impostare una partizione boot per i file di avvio ed il Linux kernel all'inizio del disco rigido (`/boot`). Questa partizione dovrebbe essere almeno di 8 Mbyte o disporre di un (1) cilindro. In linea di massima vale: se YaST propone una partizione boot si consiglia di impostarne una anche quanto si esegue il partizionamento del disco manualmente. In caso di dubbio è sempre preferibile creare una partizione di boot.

Tenete in considerazione che alcuni programmi (per lo più commerciali) installano i loro dati in `/opt`; è quindi sempre bene impostare una partizione `/opt` o creare una partizione root più generosa. Anche KDE e GNOME vengono installati sotto `/opt`.

Partizionamento con YaST

Selezionando la proposta di partizionamento nella finestra di dialogo, appare la finestra di partizionamento di YaST con i parametri attuali, che potete accettare, cambiare o rifiutare del tutto, sostituendoli con un altro assetto di partizionamento.

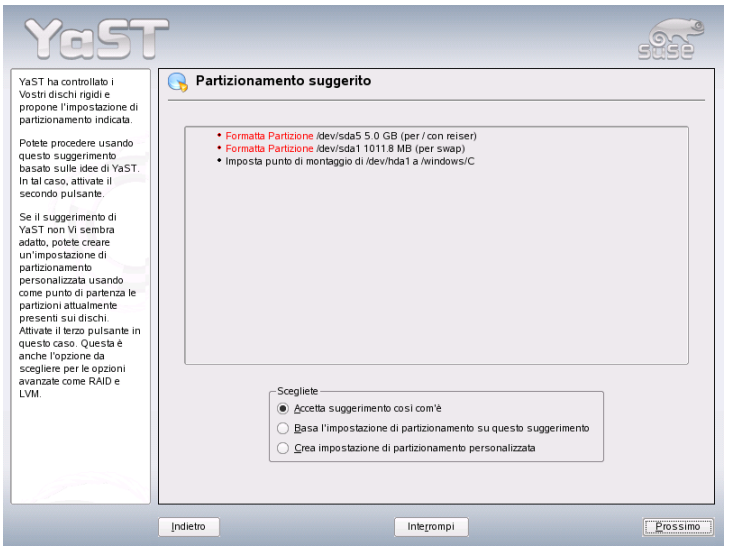

Figura 1.6: *Modificare la proposta di partizionamento*

Se cliccate su 'Accetta la proposta di partizionamento', non verrà modificato nulla. Se, invece, cliccate su 'Modifica la proposta di partizionamento', appare direttamente la finestra per esperti, che vi permette di agire su delle impostazioni in modo molto dettagliato (si veda la sezione 2.7.5 a pagina 73). Come punto di partenza troverete la proposta di YaST che può ora essere modificata.

Se cliccate poi su 'Creare partizioni personalizzate', appare innanzitutto una finestra di selezione per la scelta del disco rigido (si veda la figura 1.7 in questa pagina), con una lista dei dischi rigidi presenti nel vostro sistema. Selezionate quello su cui installare SUSE LINUX.

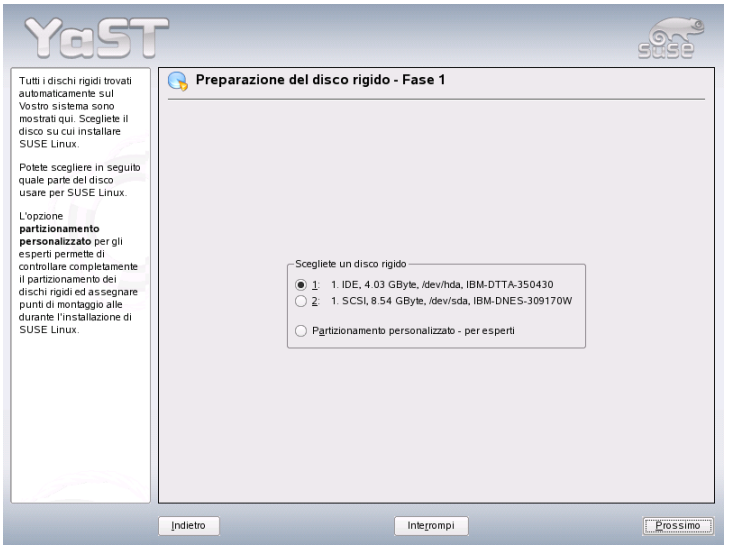

Figura 1.7: *Selezionare il disco rigido*

Una volta scelto un disco rigido, sta ancora a voi decidere se usare l''Intero disco rigido' o solo alcune partizioni (se già ve ne sono). Se viene rilevato Windows, vi verrà chiesto se intendete cancellare o ridurre la partizione Windows. A questo proposito, vi preghiamo di consultare la sezione Adattare una partizione Windows nella pagina seguente. Altrimenti giungete anche da qui alla finestra di dialogo per esperti, dove potete impostare una partizione secondo le vostre preferenze (si veda la sezione 2.7.5 a pagina 73).

Avvertimento

Usare tutto il disco rigido per l'installazione

Scegliendo 'Intero disco rigido', tutti i dati che finora risiedono sul disco verranno cancellati.

Avvertimento

Ora, YaST verifica se lo spazio è sufficiente per eseguire l'installazione del software selezionato. In caso negativo, cambierà la vostra selezione, comunicandovelo nella finestra di dialogo contenente la proposta. Se la memoria è sufficiente, YaST applicherà i vostri valori e la vostra suddivisione del disco.

Adattare una partizione Windows

Se, nell'ambito del partizionamento, è stato scelto per installare il sistema un disco rigido contenente una partizione Windows del tipo FAT o NTFS , YaST vi consente di eliminare o ridimensionare questa partizione. In questo modo, potete installare SUSE LINUX anche se sul disco rigido c'è abbastanza spazio disponibile. Quest'opzione è particolarmente utile quando il disco rigido è completamente occupato da una sola, grande partizione Windows, come per la maggior parte dei computer con un sistema preinstallato.

Se YaST rileva che sul disco rigido non vi è spazio sufficiente per installare Linux e che questo problema potrebbe essere risolto eliminando o riducendo la partizione di Windows, verrà aperta una finestra di dialogo in cui poter selezionare tra le opzioni disponibili.

Selezionando 'Cancellare completamente Windows', la partizione viene contrassegnata per essere cancellata e lo spazio liberato verrà messo a disposizione all'installazione di SUSE LINUX.

Avvertimento

Cancellare Windows

Se cancellate Windows, tenete presente che tutti i dati in Windows andranno irrimediabilmente persi al momento della formattazione.

Avvertimento

Se decidete di ridurre la partizione di Windows, interrompete prima l'installazione e caricate Windows per prepararlo al ridimensionamento. Questa misura non è indispensabile per le partizioni FAT, ma accelera il processo di ridimensionamento e lo rende più sicuro. Per le partizioni NFTS, invece, è un passaggio necessario.

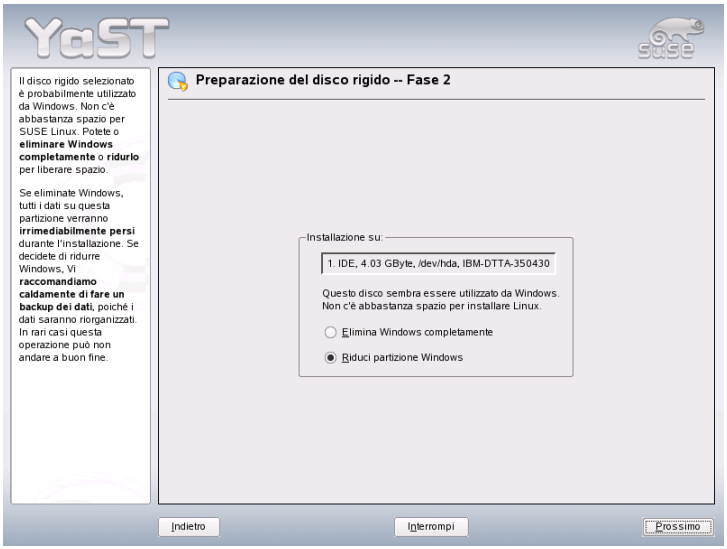

Figura 1.8: *Possibili opzioni con partizioni Windows.*

File system FAT Su Windows, avviate il programma scandisk, per assicurarvi che il file system FAT non contenga errori di concatenazione. Dopodiché, usate defrag per spostare i file all'inizio della partizione. Questo piccolo stratagemma accelererà il processo di ridimensionamento.

Se avete configurato un'ottimizzazione swap di Windows con relativo file swap, a limite superiore ed inferiore costante, si consiglia di eseguire un ulteriore passaggio preparativo. Infatti, in questo caso, il ridimensionamento potrebbe spezzettare il file swap e spargerlo per tutta la partizione di Windows. Inoltre, il file swap deve essere spostato con tutto il resto della partizione durante il ridimensionamento, cosa che rallenta il processo. Pertanto, eliminate l'ottimizzazione prima della riduzione e riconfiguratela dopo il processo.

File system NTFS Lanciate innazitutto sotto Windows i programmi scandisk e defrag, in modo da spostare i file all'inizio del disco rigido. A differenza dei file system FAT, i sistemi NFTS hanno *assolutamente* bisogno di questo accorgimento per permettere il ridimensionamento.

Importante

Ridimensionare la swap di Windows

Se il vostro sistema presenta un file swap permanente su un file system NTFS, questo file potrebbe trovarsi alla fine del disco rigido e restarci anche dopo la deframmentazione. Di conseguenza, potrebbe rivelarsi difficile ridurre sufficientemente la partizione. In questo caso, disattivate temporaneamente il file swap (la memoria virtuale) di Windows. Dopo il ridimensionamento della partizione, potete configurare di nuovo tutta la memoria virtuale che volete.

Importante

Dopo questi preparativi tornate nuovamente alla finestra di dialgo relativa al partizionamento, e selezionate 'Ridurre partizione Windows'. Dopo una breve verifica della partizione, YaST apre una nuova finestra di dialogo con una proposta di ridimensionamento della partizione di Windows.

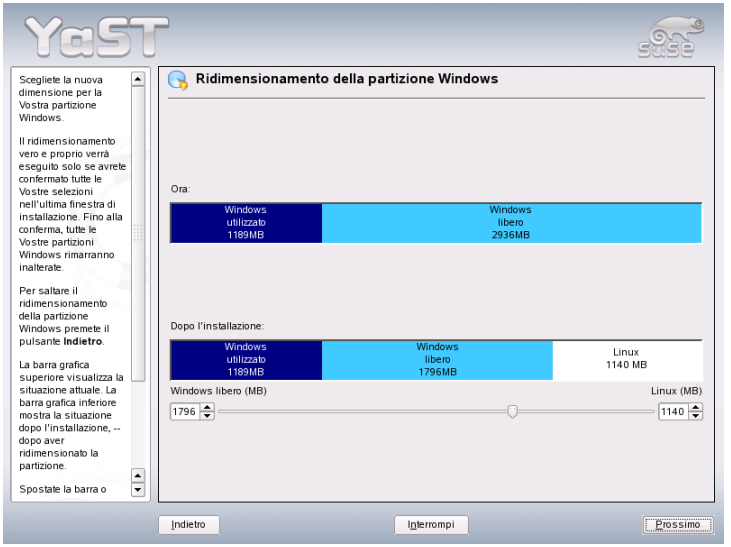

Figura 1.9: *Ridimensionare la partizione di Windows.*

YaST vi mostra quanto spazio venga occupato da Windows nel primo diagramma a barre e quanto sia ancora libero. Il secondo diagramma vi propone come suddividere il disco rigido (si veda la figura 1.9 a fronte). Potete accettare la proposta o apportare delle modifiche alla proposta azionando il cursore scorrevole.

Chiudete questa finestra di dialogo con 'Prossimo' ed i nuovi valori verranno salvati. Poi tornate alla finestra di dialogo precedente. Il processo di ridimensionamento non inizia subito, ma in un secondo tempo, subito prima di formattare il disco rigido.

Importante

Windows con file system NTFS

Le versioni di Windows NT, 2000 ed XP usano un file system di tipo NTFS. Diversamente dal FAT, il file system NTFS è (per il momento) accessibile da Linux in sola lettura. Pertanto, con NTFS potete solo leggere i vostri file Windows su Linux, ma non modificarli. Se desiderate modificare i vostri file di Windows e pensate di poter rinunciare al file system NTFS, potete reinstallare Windows con un file system FAT 32. In questo modo, avete un accesso completo ai vostri dati Windows anche da SUSE LINUX.

Importante

1.5.5 Software

SUSE LINUX contiene una vasta scelta di pacchetti per le applicazioni più disparate. E per risparmiarvi la fatica di andare a cercare quelli che fanno al vostro caso, SUSE LINUX vi offre una preselezione di applicazioni, raccolte in tre tipi di sistemi di dimensioni diverse. YaST analizza le risorse del vostro sistema e propone l'installazione del sistema più adatto alle caratteristiche del vostro computer.

Sistema minimale (consigliabile solo per usi particolari)
: In questo caso viene installato solo il sistema operativo accanto ad una serie di servizi. È esclusa l'interfaccia grafica, per operare sul sistema si ha a disposizione solo la console ASCII. Questo tipo di installazione è adatta per applicazioni server, che non prevedono interazione diretta con l'utente.

Sistema grafico minimale (senza KDE o GNOME)
: Se volete rinunciare a KDE o GNOME oppure non avete spazio a sufficienza potete decidervi per questo tipo di installazione. Questo sistema

comprende una interfaccia grafica elementare con un window manager. Può essere utilizzato con tutti i programmi che dispongano di una propria interfaccia grafica. Non comprende l'installazione di programmi Office.

Sistema standard con GNOME e pacchetto Office
Si tratta dell'installazione più voluminosa tra i sistemi di base: contiene il desktop GNOME e la maggior parte dei programmi di GNOME e le applicazioni Office.

Sistema standard con KDE e pacchetto Office
Contiene il desktop KDE e la maggior parte dei programmi di KDE e le applicazioni Office.

Se nella finestra delle proposte cliccate su 'Software', appare una finestra di dialogo dove potete selezionare uno dei sistemi di base di cui sopra. Con 'Selezione dettagliata', potete anche avviare il modulo di installazione del software (il "package manager") e aggiungere o eliminare applicazioni dai pacchetti da installare (si veda la figura 1.10 in questa pagina).

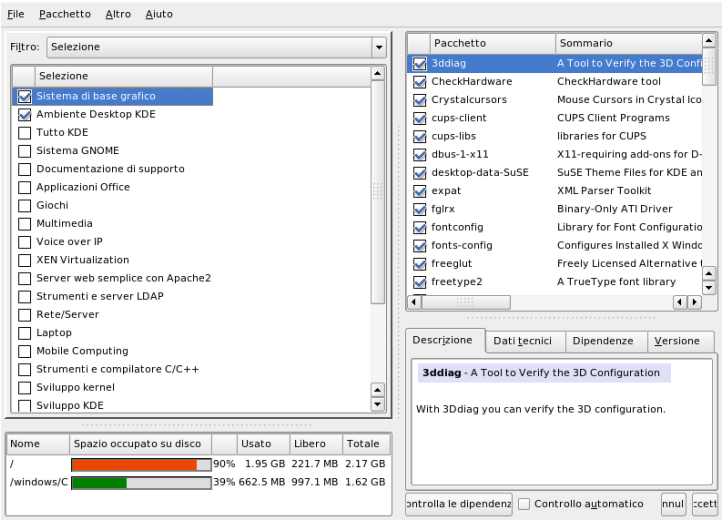

Figura 1.10: *Installare o eliminare del software con il gestore pacchetti di YaST (package manager)*

Modificare la preselezione dei pacchetti da installare

Con il “sistema predefinito”, non è solitamente necessario cambiare la composizione dei pacchetti, in quanto questo sistema contiene una selezione di software completa che risponde alle richieste più diffuse e comuni. Tuttavia, se desiderate di intervenire manualmente, ricorrete all’assistenza del package manager. Il package manager vi offre dei cosiddetti "filtri", che raggruppano i pacchetti di SUSE LINUX in diverse selezioni.

In alto a sinistra, sotto la riga dei menu, trovate la finestra dei filtri. All’avvio, viene visualizzato il filtro ‘Selezioni’. Questo filtro raggruppa i pacchetti di applicazioni a seconda della loro funzione (multimedia, office, ecc.). I gruppi così formati dal filtro vi vengono mostrati sotto la lista dei filtri: alcuni di questi gruppi sono già contrassegnati, perché appartengono al tipo di sistema che avete selezionato. Per escludere o aggiungere gruppi di software, cliccate sulla casella corrispondente.

Nella finestra sulla destra, vedete una lista dei pacchetti singoli appartenenti alla selezione attuale. Tutti i pacchetti hanno uno “stato” che viene indicato con un simbolo all’inizio della riga, in una piccola finestra di stato. In questa fase dell’installazione, ci interessano soprattutto gli stati ‘Installare’ (casella con segno di spunta) e ‘Non installare’ (casella vuota). Anche in questo modulo, potete modificare i pacchetti a seconda delle vostre esigenze, cliccando sul simbolo alla sinistra del pacchetto fino a avere lo stato desiderato (installare o non installare). In alternativa, cliccate con il tasto destro del mouse sulla riga dei pacchetti: apparirà un menu contestuale con tutti gli stati possibili. Gli altri stati verranno descritti nell’introduzione di questo modulo nella sezione 2.2.1 a pagina 40.

Altri filtri

Cliccando su ‘Filtri’, otterrete una lista degli altri filtri che vi aiuteranno a visualizzare i pacchetti in modo più strutturato. Interessante è anche la selezione sulla base dei ‘Gruppi di pacchetti’. Con questo filtro, i pacchetti vengono raggruppati in base a dei temi e visualizzati a sinistra, in una struttura ad albero. Più gruppi di pacchetti ("temi") aprite, più minuziosa e mirata sarà la scelta di pacchetti che vi verrà mostrata nella lista a destra.

Per cercare un determinato pacchetto, cliccate su ‘Cerca’. Questa funzione viene illustrata anche nella sezione 2.2.1 a pagina 40.

Dipendenze e conflitti

Come per tutti i sistemi operativi bisogna fare attenzione a non installare contemporaneamente determinati tipi di pacchetti. L’installazione di pacchetti non

perfettamente compatibili tra loro potrebbe destabilizzare il sistema. Il sistema vi avverte di eventuali conflitti o dipendenze irrisolte tra pacchetti selezionati da dover installare. Se installate SUSE LINUX per la prima volta o non vi è chiaro il significato di questi avvertimenti, vi preghiamo di consultare la sezione 2.2.1 a pagina 40, dove troverete informazioni dettagliate sull'utilizzo del package manager ed una breve introduzione al tema del modo di organizzare il software su Linux.

Avvertimento

La selezione standard che vi viene proposta è adatta sia al novizio che all'utente più esperto, in quanto elaborata sulla base di dati empirici. Pertanto, di solito non è necessario modificarla. Se decidete di aggiungere o escludere dei pacchetti dall'installazione, dovete essere sempre sicuri su cosa state facendo. Soprattutto nell'eliminare dei pacchetti, fate attenzione agli avvertimenti del programma e non eliminate mai dei pacchetti appartenenti al sistema di base Linux.

Avvertimento

Uscire dalla selezione del software

Se siete soddisfatti della selezione e non vi sono dei conflitti o delle dipendenze di pacchetti da risolvere, salvate le vostre modifiche con 'Accetta' e uscite dal modulo. A questo punto le modifiche vengono solo salvate, essa verranno applicate quando verrà inizializzato il processo di installazione vero e proprio.

1.5.6 Configurazione del boot

La configurazione del boot loader viene normalmente impostata da YaST durante l'installazione del sistema. Solitamente, non è necessario apportare delle modifiche, a meno che il vostro sistema non presenti caratteristiche particolari.

Ad esempio, potete modificare la configurazione del boot in modo da avviare il sistema da un dischetto speciale di caricamento. È un'opzione consigliabile in tutti quei casi in cui sia un altro sistema operativo ad essere usato più spesso e non si desideri cambiare il suo meccanismo di boot. Non dovrebbe comunque essere necessario, dal momento che YaST configura il boot loader in modo che possano coesistere diversi sistemi operativi da poter selezionare durante la fase di avviamento del sistema. Un'altra possibilità consiste nel modificare la configurazione in modo da cambiare l'ubicazione del boot loader sul disco rigido.

Per cambiare la configurazione del boot proposta da YaST, selezionate 'Avvio sistema'. Appare una finestra di dialogo che vi permette di intervenire sulla procedura di caricamento del sistema (vedete il sezione 8.4 a pagina 190). E' consigliabile avere una certa esperienza prima di intervenire sulla configurazione del boot.

1.5.7 Fuso orario

In questa finestra (si veda la figura 1.11 in questa pagina), impostate il parametro 'Imposta orologio su' su `Ora locale` o `UTC` (Universal Time Coordinated) . La vostra scelta dipenderà dalle impostazioni dell'orologio hardware (BIOS): se è impostato su `GMT`, che corrisponde a UTC, SUSE LINUX gestisce automaticamente il passaggio dall'ora solare a quella legale e viceversa.

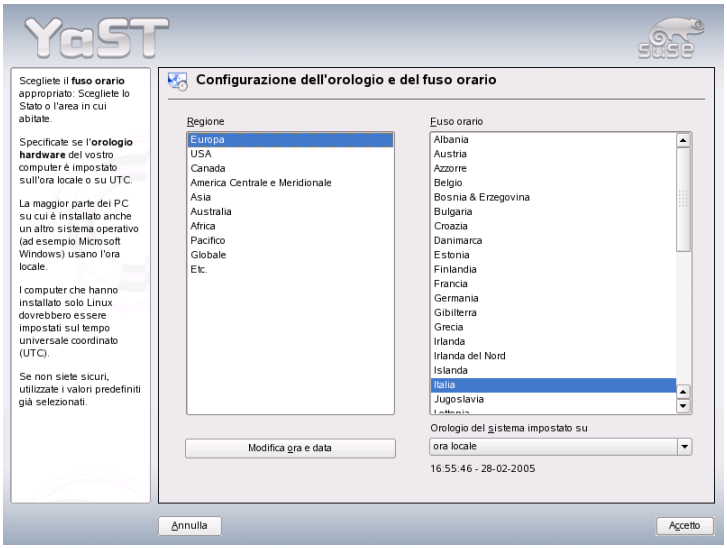

Figura 1.11: *La selezione del fuso orario*

1.5.8 Lingua

La lingua viene selezionata all'inizio dell'installazione (si veda la sezione 1.3 a pagina 8). Se volete modificarla, usate questo modulo; potete selezionare delle lingue aggiuntive da installare. Nella parte superiore di questa finestra potete selezionare la lingua primaria. Sarà la lingua ad esser abilitata a installazione avvenuta. Se volete, potete anche adattare la vostra tastiera e le vostre impostazioni riguardanti il fuso oraio alla lingua primaria spuntando le rispettive caselle. Inoltre sussiste la possibilità di impostare la lingua per l'utente `root` tramite il pulsante 'Dettagli'. Potete scegliere tra queste tre opzioni:

ctype only Per l'utente `root` trova applicazione il valore della variabile `LC_CTYPE` nel file `/etc/sysconfig/language`. Tramite questa variabile si imposta la localizzazione delle chiamate di funzioni per le varie lingue.

yes `root` usa le stesse impostazioni linguistiche dell'utente locale.

no Le impostazioni della lingua per `root` non sono influenzate dalla selezione della lingua. Tutte le variabili di `locale` verranno azzerate.

Alcuni amministratori di sistema preferiscono che l'account di `root` non supporti UTF-8. In tal caso deselezionate 'Usa codifica UTF-8'.

L'elenco in basso della finestra consente la selezione di ulteriori lingue da installare. Per le lingue selezionate in questo elenco YaST verifica la presenza di pacchetti specifici di una lingua per i pacchetti parte della selezione di software attuale. In caso affermativo i pacchetti in questione verranno installati.

Per chiudere la finestra di configurazione, cliccate su 'Accetto'. Per annullare le vostre modifiche, cliccate su 'Rifiuta'.

1.5.9 Eseguire l'installazione

Per accettare i valori proposti nella finestra, cliccate su 'Avanti'. La selezione proposta verrà applicata con tutte le vostre modifiche e arriverete alla finestra di dialogo verde di conferma. Se ora cliccate su 'Sì', ha inizio l'installazione così come l'avete impostata. Il processo di caricamento dei pacchetti può durare tra i 15 e i 30 minuti. Una volta installati i pacchetti, YaST avvia il sistema installato prima di poter proseguire con la configurazione dell'hardware e dei servizi.

1.6 Concludere l'installazione

Ad installazione conclusa, resta solo da impostare una password per l'amministratore del sistema (l'utente `root`). Dopodiché, potrete configurare anche l'accesso a Internet e la connessione di rete. In questo modo, potrete utilizzare gli aggiornamenti del software già durante l'installazione e, eventualmente, configurare anche un server di autenticazione per l'amministrazione centralizzata degli utenti sulla rete locale. Infine, configurate l'hardware collegato al vostro sistema.

1.6.1 La password di root

root è il nome del superutente, dell'amministratore del sistema. `root` può fare tutto quello che non è concesso all'utente normale. Può modificare l'assetto configurativo del sistema, installare dei programmi o configurare nuovo hardware. `root` può risolvere il problema quando l'utente ha dimenticato la sua password o sbloccare programmi in panne. In generale, si dovrebbe agire come `root` solo per amministrare, manutenere e riparare il sistema. Per gli altri casi non è consigliabile agire da `root`, dato che con un singolo comando erroneo potreste cancellare involontariamente numerosi file di sistema in modo irrecuperabile.

Per configurare la password di `root`, occorre digitarla due volte (si veda la figura 1.12 nella pagina seguente). Non dimenticatela, dato che è impossibile recuperarla.

Avvertimento

L'utente root

L'utente `root` dispone di tutti i permessi e può eseguire ogni tipo modifica al sistema. Senza la password di `root`, non è possibile eseguire l'amministrazione del sistema.

Avvertimento

1.6.2 Configurazione della rete

Il prossimo passo consiste nel connettere il vostro sistema con il resto del mondo, configurando una scheda di rete, ISDN, modem o DSL. Approfittatene se disponete di questo tipo di hardware: nel proseguio YaST potrà scaricare dalla rete Internet degli aggiornamenti per SUSE LINUX che potranno essere integrati già durante il processo di installazione.

Figura 1.12: *Impostare la password di root*

Per configurare il vostro hardware di rete, consultate le rispettive sezioni della sezione 22.4 a pagina 415. Altrimenti selezionate 'Salta configurazione' e proseguite con 'Prossimo'. Potrete configurare la vostra scheda di rete anche in un secondo momento.

1.6.3 Configurazione del firewall

Non appena connettete in rete il vostro sistema, sull'interfaccia configurata viene attivato automaticamente un firewall. Le impostazioni del firewall vengono visualizzate nella finestra della configurazione della rete. Ad ogni modifica apportata all'interfaccia o alla configurazione dei servizi viene aggiornata automaticamente la proposta di configurazione per il firewall. Se volete adattare le impostazioni generate automaticamente, cliccate su 'Modifica' → 'Firewall'. Nella finestra che verrà visualizzata a questo punto stabilite se il firewall debba essere avviato o meno. Se non volete inizializzare il firewall, abilitate la relativa opzione e uscite dalla finestra. Se intendete avviare e configurare il firewall, premete su 'Prossi-

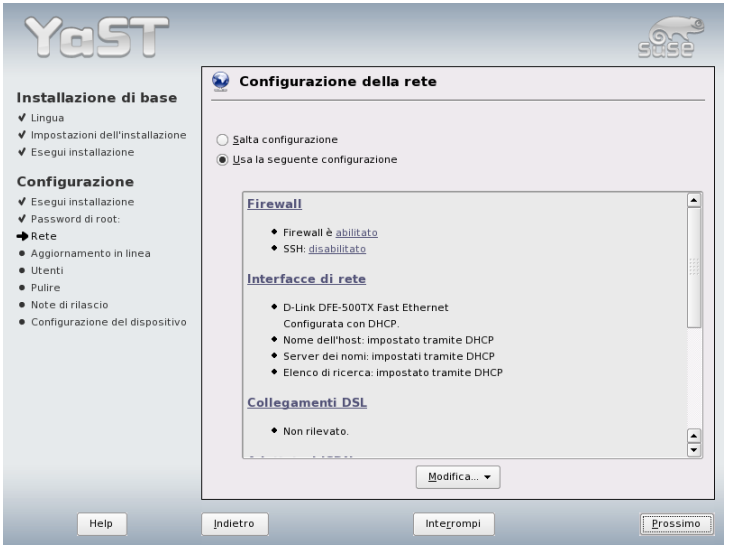

Figura 1.13: *Configurazione dei dispositivi di rete*

mo' per avere una sequenza di finestre simile a quella descritta nella sezione Configurazione con YaST a pagina 609.

1.6.4 Testare la connessione Internet

Se avete configurato una connessione Internet, potete testarla. YaST si collega al server di SUSE e ne approfitta per controllare se ci sono degli aggiornamenti per la vostra versione di SUSE LINUX. In caso affermativo potrete scaricarli e integrarli subito nel vostro sistema. Inoltre vengono scaricate le ultime note di rilascio (release notes) dal server SuSE, che potrete leggere una volta terminato il processo di installazione.

Se non desiderate testare la connessione, cliccate su 'Salta test' e poi su 'Prossimo'. Chiaramente, non verranno rilevati né gli aggiornamenti né le note di rilascio.

Figura 1.14: *Testare la connessione Internet*

1.6.5 Scaricare gli aggiornamenti del software

Se il collegamento con il server SUSE ha funzionato, YaST vi permette di eseguire un cosiddetto "Online-Update". Questo significa che il programma scarica subito dal server SUSE le ultime patch che risolvono eventuali errori o problemi di sicurezza.

Importante

Scaricare gli aggiornamenti

Scaricare gli aggiornamenti a volte richiede parecchio tempo, a seconda, naturalmente, dalla velocità della vostra connessione Internet e dalle dimensioni degli aggiornamenti.

Importante

Per eseguire subito un aggiornamento, selezionate ‘Esegui update ora’ e cliccate su ‘OK’. Si apre la finestra di dialogo "Online-Update", dove potrete vedere tutte le patch a vostra disposizione, da poter scegliere ed applicare. Vi preghiamo an-

che di leggere la sezione 2.2.3 a pagina 49. Gli aggiornamenti possono essere installati anche in un secondo momento. Se preferite farlo più tardi, selezionate 'Salta update' e cliccate su 'OK'.

1.6.6 Autenticazione degli utenti

Se durante il processo di installazione è stato già configurato l'accesso di rete, potrete scegliere ora tra due metodi per amministrare gli utenti del sistema appena installato.

Amministrazione utenti locali Gli utenti vengono amministrati localmente sul sistema installato. Un'opzione consigliabile per tutte le postazioni di lavoro standalone. I dati degli utenti vengono amministrati in questo casi tramite il file locale `/etc/passwd`.

LDAP L'amministrazione degli utenti per tutti i sistemi della rete avviene centralmente sul server LDAP.

NIS L'amministrazione degli utenti per tutti i sistemi della rete avviene centralmente sul server NIS.

Samba L'autenticazione SMB trova spesso applicazione in reti eterogenee Linux/Windows.

Se ci sono tutti i requisiti, YaST visualizza una finestra di dialogo per selezionare il metodo più adatto al vostro caso (si veda la figura 1.15 nella pagina seguente). Se non c'è una connessione di rete, potete creare in ogni caso degli utenti locali.

1.6.7 Configurare un host come client NIS

Se avete deciso di amministrare gli utenti tramite NIS, è venuto il momento di configurare un client NIS. In questo manuale, ci limiteremo a descrivere la configurazione del client, per delle informazioni sulla configurazione del server NIS con YaST rimandiamo alla capitolo 25 a pagina 467.

Nella finestra successiva (si veda la figura 1.16 a pagina 31) selezionate innanzitutto se il client NIS dispone di un'indirizzo IP statico o se debba ottenere un indirizzo IP tramite DHCP. Se selezionate DHCP non potete indicare un indirizzo IP di un server o dominio NIS, visto che anche questi dati vengono assegnati tramite DHCP. Per ulteriori informazioni su DHCP, leggete la capitolo 27 a pagina 479. Se

Figura 1.15: *Autenticazione degli utenti*

il client dispone di un indirizzo IP statico, il dominio e server NIS vanno immessi manualmente.

Per rilevare dei server NIS che inviano dei broadcast, selezionate la rispettiva opzione. Potete anche indicare una serie di domini e specificare un dominio di default. Ad ognuno dei domini potete assegnare più server con funzionalità broadcast, cliccando su 'Modifica'.

Per impedire che un altro sistema possa scoprire quale server utilizza il vostro client, abilitate nelle impostazioni per esperti l'opzione 'Rispondi solo all' host locale'. Se, invece, selezionate l'opzione 'Server malfunzionante', verranno accettate anche le risposte di un server su una porta non privilegiata. Per maggiori dettagli, consultate la pagina di manuale di `ypbind`.

1.6.8 Creare utenti locali

Se decidete di non utilizzare un server di autenticazione preposto all'autenticazione degli utenti, create gli utenti locali. I dati di questi utenti (nome, login, password, ecc.) vengono salvati ed amministrati direttamente sul sistema.

Figura 1.16: *Configurazione client NIS*

Linux permette a più utenti di lavorare contemporaneamente sul medesimo sistema. Ogni utente deve disporre di uno “user account” che gli permette di eseguire il login. La presenza degli account offre un’ottimo livello di sicurezza operativa. Infatti, agli utenti normali non è permesso di modificare o eliminare dei file di sistema importanti. I dati di ogni utente sono protetti dall’accesso da parte degli altri utenti, che non possono né visualizzarli né modificarli. Inoltre, ogni utente può personalizzare il suo ambiente di lavoro, che troverà invariato ogni volta che si immetterà nel sistema.

La configurazione di uno “user account” si esegue nella finestra riportata nella figura 1.17 nella pagina seguente. Inserite il vostro nome e cognome ed inventatevi uno "username" con cui immettervi nel sistema ("login"). Se non vi viene in mente niente, fatevene proporre uno con il pulsante ‘Proponi’.

Infine, va inserita una password per l’utente (due volte, per evitare degli errori di battitura). Lo username comunica al sistema *chi* siete. La password gli garantisce che lo siate *veramente*.

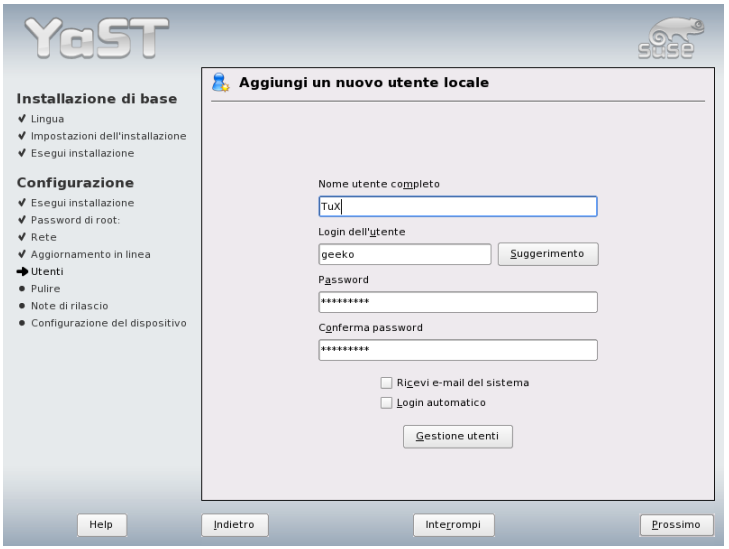

Figura 1.17: *Impostare il nome utente e password*

Avvertimento

Nome utente e password

Tenete ben in mente il nome utente e la password, dal momento che ne avrete bisogno per immettervi nel sistema.

Avvertimento

Una password sicura dovrebbe essere composta da almeno 5 fino a 8 caratteri. In linea di principio, la lunghezza massima di una password può arrivare fino a 128 caratteri. Tuttavia, per l'identificazione, vengono utilizzati solo i primi otto, a meno che non abbiate installato dei moduli appositi. Si distingue tra lettere maiuscole e minuscole. Potete usare i numeri da 0 a 9 e caratteri speciali (7-bit ASCII), ma non le lettere accentuate.

L'utente locale può anche scegliere tra due opzioni:

'Messaggi di sistema recapitati tramite e-mail'
Se selezionate questa opzione, il sistema vi recapita i messaggi dei servizi

di sistema. Questi messaggi, normalmente, vengono inviati solo all'amministratore, l'utente `root`. Tuttavia, dal momento che ci si dovrebbe solo immettere come `root` solo in casi particolari, si consiglia di indicare l'utente che utilizza il sistema con maggiore frequenza.

'Login automatico' Questa opzione è disponibile solo se usate il desktop di KDE come default; essa permette all'utente attuale di accedere al sistema direttamente, subito dopo l'avvio del sistema stesso. Scegliete questa opzione se siete gli unici ad usare il sistema.

Avvertimento

Login automatico

Con il login automatico, dopo l'avvio del sistema, non vi è alcuna autenticazione. Questa opzione, pertanto, *non* è consigliabile se il computer contiene dati sensibili e se viene usato da più persone.

Avvertimento

1.6.9 Note di rilascio

Una volta configurata l'autenticazione dell'utente, vi vengono mostrate le note di rilascio. Vi consigliamo di leggerle, dal momento che contengono informazioni importanti, non ancora disponibili al momento della stampa dei manuali. Se disponete di una connessione Internet che avete testato connettendovi al server di SUSE, viene scaricata l' ultima versione delle note di rilascio.

1.7 Configurazione dell'hardware

E per finire, YaST presenta una finestra che vi permette di configurare la scheda grafica nonché altri componenti hardware connessi al sistema come la stampante o la scheda audio. Cliccando sui singoli componenti potete avviare la configurazione dell'hardware. YaST rileverà e configurerà il vostro hardware per lo più automaticamente.

La configurazione dei dispositivi periferici può essere fatta in un secondo tempo, ma vi consigliamo comunque di configurare almeno i parametri della scheda grafica. I valori proposti da YaST nella maggior parte dei casi possono essere accettati. Eppure, in ambito di risoluzione e profondità cromatica dello schermo,

Figura 1.18: *Configurazione dei componenti di sistema*

i gusti differiscono da utente a utente. Per modificare questa proposta, selezionate il punto 'Scheda grafica'. Le impostazioni di questa finestra sono descritte più dettagliatamente nella sezione 11.1 a pagina 224. Dopo aver scritto i dati di configurazione, nella finestra di dialogo conclusiva di YaST potrete terminare l'installazione di SUSE LINUX con 'Fine'.

1.8 Login grafico

A questo punto Il processo di installazione di SUSE LINUX è concluso. Se per l'amministrazione degli utenti in locale avete abilitato il login automatico potete entrare nel sistema senza dover prima eseguire il login. Altrimenti sul vostro schermo appare il login grafico come mostrato nella figura 1.19 a fronte). Digitate il vostro nome utente e la password per eseguire il login.

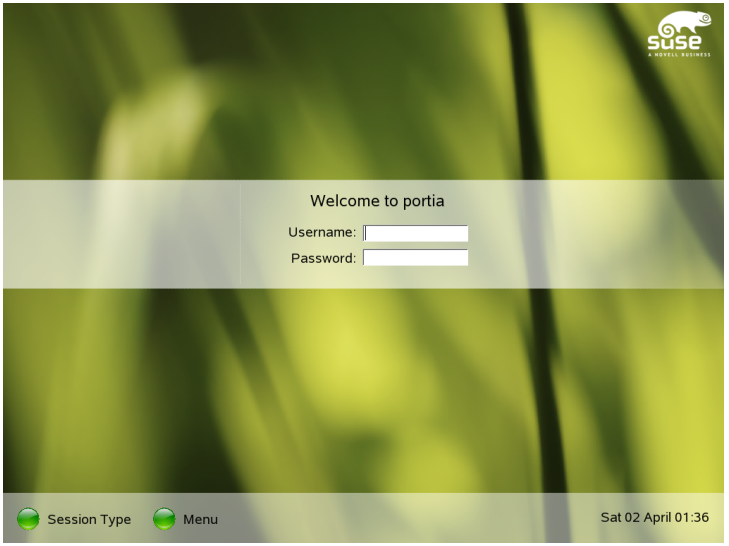

Figura 1.19: *Schermata di login di KDM*

Configurazione del sistema con YaST

Avete già fatto la conoscenza di YaST (ingl. Yet another Setup Tool) durante il procedimento di installazione. YaST è lo strumento di configurazione per eccellenza di SUSE LINUX. Questo capitolo descrive la configurazione del sistema con YaST. Potete configurare in modo semplice e veloce la maggior parte dei componenti hardware, la superficie grafica, l'accesso a Internet, le impostazioni di sicurezza, nonché amministrare gli utenti, installare software, aggiornare il sistema e ottenere delle informazioni inerenti al sistema stesso. Nel presente capitolo tratteremo anche come lavorare con YaST nel modo di testo.

La configurazione del sistema con YaST ha luogo tramite diversi moduli specifici. A seconda della piattaforma hardware ed il software installato potete lanciare YaST in vario modo.

Con KDE o GNOME il centro di controllo di YaST si avvia tramite il menu SUSE ('Sistema' → 'YaST'). Inoltre, il centro di controllo di KDE include i singoli moduli di configurazione. L'inizializzazione di YaST richiede la password di root, visto che YaST richiede i permessi di root per poter apportare delle modifiche ai file di sistema.

Dalla linea di comando YaST si avvia tramite la sequenza di comandi `su` (per diventare `root`) e `yast2`. Se volete avviare la versione testo di YaST, immettete `yast` al posto di `yast2`. Utilizzate il comando `yast` anche per avviare il programma da una delle console virtuali.

Suggerimento

Per cambiare la lingua di YaST, andate nel centro di controllo di YaST e cliccate su 'Sistema' → 'Scegliete la lingua'. Selezionate la vostra lingua, chiudete il centro di controllo di YaST, eseguite quindi il log out e subito dopo il log in. Al prossimo avvio di YaST avrete abilitato la lingua richiesta.

Suggerimento

Nel caso di piattaforme hardware che non supportano un proprio display oppure ai fine dell'amministrazione remota, lanciate YaST da remoto. Aprite una console sull'host sul quale visualizzare YaST ed immettete il seguente comando per entrare come `root` nel sistema da configurare e per reindirizzare l'output dell' X server sul vostro terminale: `ssh -X root@<nome del sistema>` Non appena avete eseguite il login tramite SSH, immettete `yast2` per avviare YaST nel modo grafico.

Per avviare YaST nel modo di testo, utilizzate `ssh root@<sistema-da-configurare>` per creare la connessione ed avviate YaST con il comando `yast`.

2.1 Il centro di controllo di YaST

Se avviate YaST nel modo grafico si apre innazitutto il centro di controllo di YaST (si veda la figura 2.1 nella pagina successiva). Sulla sinistra vi sono le categorie

'Software', 'Hardware', 'Dispositivi di rete', 'Servizi di rete', 'Sicurezza e Utenti', 'Sistema' e 'Vari'. Cliccando su una delle icone, ne verrà mostrato il contenuto sulla destra. Se ad esempio cliccate su 'Hardware' e sulla destra su 'Audio', si apre una finestra in cui poter configurare la scheda audio. Il processo di configurazione si compone di diversi passaggi, per cui bisogna cliccare su 'Prossimo' per approdare alla fase successiva dell'iter configurativo.

Sulla sinistra troverete delle spiegazioni riguardo ad ogni maschera. Per ricevere dell'aiuto nei moduli sprovvisti di tali illustrazioni, vi è il tasto F1 o selezionate 'Aiuto' nel menu. Una volta inseriti i dati necessari, potete salvare e chiudere la configurazione cliccando su 'Fine'.

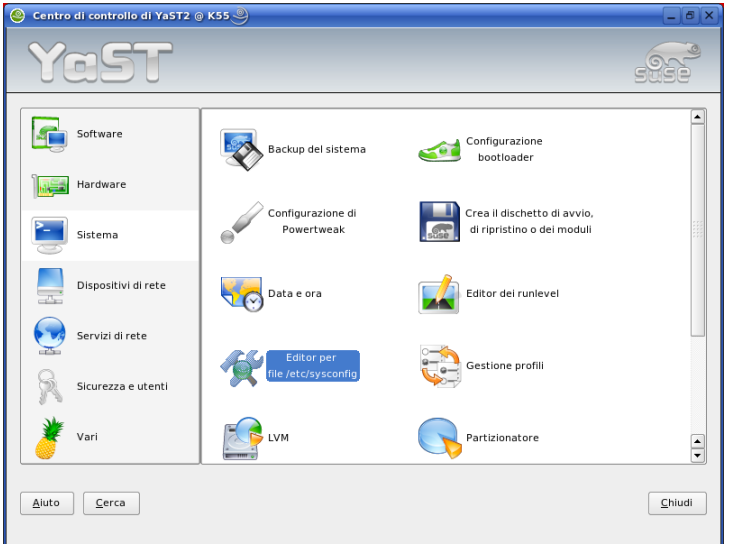

Figura 2.1: *Il centro di controllo di YaST*

2.2 Software

2.2.1 Installare o eliminare software

Questo modulo vi permette di installare, disinstallare o attualizzare il software del sistema. Su Linux, il software è disponibile sotto forma di pacchetti. Ogni pacchetto contiene tutto quello che serve al funzionamento di un determinato programma, vale a dire, oltre al programma stesso, i rispettivi file di configurazione e la relativa documentazione. Di solito è disponibile inoltre un pacchetto contenente i file sorgenti del programma. Questi file non sono necessari per l'esecuzione del programma, ma sono essenziali se si desidera installare una versione personalizzata di un programma.

Alcuni pacchetti dipendono da altri. Ciò vuol dire che il software di un determinato pacchetto può funzionare correttamente solo in presenza di un altro pacchetto ("dipendenza"). Inoltre, alcuni pacchetti si possono installare solo se non sono già presenti altri pacchetti, a volte perché la loro installazione richiede un determinato tipo di tool. Quindi questo tipo di pacchetti va installato in un ordine ben preciso. Vi sono poi alcuni pacchetti con la medesima funzione o con una simile . Se questi pacchetti attingono alle stesse risorse del sistema, non possono essere installati assieme ("conflitto"). Dipendenze e conflitti possono verificarsi sia tra due pacchetti sia tra una serie di pacchetti e assumere contorni davvero complessi, specialmente quando il tutto viene reso ancora più complicato dal fatto che solo determinate versioni di pacchetti armonizzano bene.

Tutto questo va tenuto presente quando si installa o si elimina del software. Fortunatamente YaST offre un tool davvero efficente a tal scopo, il modulo per l'installazione del software ovvero il package manager. Il package manager analizza all'avvio il sistema e rivela i pacchetti installati. Nel momento in cui selezionate ulteriori pacchetti da installare, il package manager verifica automaticamente la presenza di eventuali dipendenze e seleziona i pacchetti richiesti (per la risoluzione delle dipendenze). Se selezionate dei pacchetti in conflitto tra loro il package manager propone una soluzione (risoluzione di conflitti). Se disponete inavvertitamente la cancellazione di un pacchetto richiesto da altri pacchetti già installati, il programma vi avverte della dipendenza con tanto di dettagli e proposta di soluzione.

A parte questi aspetti puramente tecnici, il package manager vi offre anche un elenco strutturato dei pacchetti di SUSE LINUX: in questa lista, i pacchetti sono a loro volta raggruppati in base a dei criteri.

Il package manager

Per modificare la selezione di software del vostro sistema con il package manager, andate nel centro di controllo di YaST e selezionate il modulo 'Installare/togliere i pacchetti'. Si apre la finestra di dialogo del package manager (si veda la figura 2.2 in questa pagina). La finestra del package manager si divide in aree tematiche. Potete modificare la dimensione di ogni area cliccando sulle linee divisorie delle finestre e quindi spostandole. Nelle pagine seguenti tratteremo il contenuto e il modo di utilizzare queste aree.

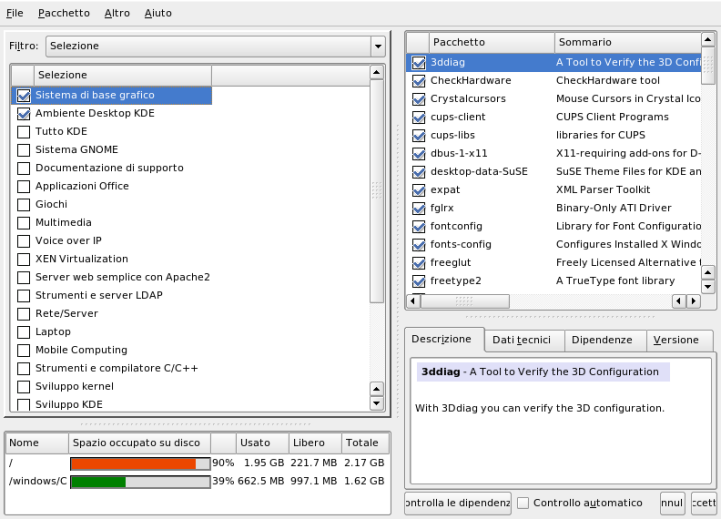

Figura 2.2: *YaST: il package manager*

La finestra dei filtri

Selezionare individualmente ogni pacchetto da installare richiederebbe una sacco di tempo. Il package manager vi offre pertanto diverse utili categorie di pacchetti. La finestra dei filtri è la sezione a sinistra, sotto la barra dei menù, e serve a gestire e visualizzare i diversi filtri. In alto, vedete il box di selezione dei filtri: quanto mostrato in questo box determina il contenuto visualizzato nella parte inferiore della finestra dei filtri. Cliccate sul box di selezione dei filtri per avere un elenco completo dei vari filtri disponibili.

Il filtro delle selezioni Appena avviate il package manager, si attiva anche il filtro 'Selezione'. Questo filtro raggruppa i pacchetti a seconda della loro funzione, ad esempio "Multimedia" o "Office". Ciò che compone il filtro 'Selezione' viene visualizzato sotto il box di selezione dei filtri. Cliccando sulla casella di stato che precede i pacchetti potete cambiarne lo stato. Cliccando con il tasto destro del mouse su di una selezione potete cambiare direttamente lo stato della selezione tramite un menu di contesto. La finestra dei pacchetti, a destra, contiene una lista dei pacchetti contenuti nella selezione evidenziata. In questa finestra, potete selezionare e deselezionare i pacchetti singolarmente.

Il filtro dei gruppi di pacchetti Vi è anche il filtro dei 'Gruppi di pacchetti' che raggruppa i pacchetti secondo criteri tecnici. Questo filtro è consigliato ad utenti già più esperti di SUSE LINUX. I pacchetti vengono visualizzati a sinistra in una struttura ad albero, suddivisi in "Applicazioni", "Sviluppo", "Hardware", ecc. Quanto più vi addentrate nella struttura ad albero, tanto più dettagliata sarà la selezione dei pacchetti. In questo caso, la lista dei pacchetti nella finestra sulla destra diventa sempre più breve e mirata.

Questo filtro vi permette anche di visualizzare *tutti* i pacchetti, in ordine alfabetico senza alcuna categorizzazione: cliccate in tal caso su 'zzz Tutti'. Visto che SUSE LINUX contiene moltissimi pacchetti potrà volerci un po' di tempo prima che venga visualizzato per interno tale elenco quasi interminabile.

Cerca Il metodo più semplice di trovare un pacchetto è rappresentato dalla funzione 'Cerca'. Con questa funzione, potete affinare i filtri tramite ulteriori criteri di ricerca, di modo che, alla fine, la ricerca viene ristretta ad un solo pacchetto in particolare. Inserite una parola chiave e selezionate, tramite le caselle, in che modo debba avvenire la ricerca (per via del nome, della descrizione o anche delle dipendenze tra pacchetti). Gli esperti possono focalizzare la ricerca tramite dei segnaposto o espressioni regolari ed eseguire una ricerca mirata delle dipendenze nei campi "Fornisce" e "Richiede". I programmatori che scaricano i sorgenti da Internet ricorrono a questo metodo per verificare ad esempio quale pacchetto contenga la libreria necessaria ai fini della compilazione del pacchetto.

Suggerimento

Ricerca avanzata nel package manager

Oltre alla funzione 'Cerca', tutte le liste del package manager comprendono anche una funzione di ricerca veloce. Basta inserire le prime lettere del nome di un pacchetto ed il cursore passa al primo pacchetto della lista il cui nome inizia con questo carattere (il cursore deve trovarsi nella lista, cliccateci).

Suggerimento

Lingue Per alcuni pacchetti di SUSE LINUX vi sono dei pacchetti specifici per determinate lingue, tipo la traduzione della localizzazione dei programmi, documentazione e font. Questo filtro mostra un elenco di lingue supportate da SUSE LINUX nella finestra a sinistra. Se ne selezionate una, la finestra sulla destra mostra i pacchetti disponibili per la lingua selezionata. Tra questi, ai fini dell'installazione vengono selezionati automaticamente tutti i pacchetti richiesti dalla vostra selezione di software attuale.

Nota

Eventualmente i pacchetti specifici per una lingua dipendono da altri pacchetti, quindi il package manager in alcuni casi selezionerà ulteriori pacchetti da includere nel processo di installazione.

Nota

Sommario dell'installazione Dopo aver selezionato dei pacchetti da installare, aggiornare o eliminare, tornate alla finestra della selezione dei filtri per farvi mostrare un riassunto di quanto selezionato. Il riassunto serve a mostrare cosa succederà con i vari pacchetti una volta che abbiate cliccato su 'Accetto'. Selezionando le caselle a sinistra, potete filtrare i pacchetti da visualizzare nella finestra dei pacchetti singoli. Per verificare, ad esempio, quali pacchetti siano già installati, disattivate tutte le caselle dopo aver avviato il package manager, fatta eccezione per 'Mantieni'.

Anche lo stato dei pacchetti nella finestra dei pacchetti si lascia modificare nella maniera consueta. A volte un determinato pacchetto non corrisponde più ai criteri di ricerca. Per eliminare un pacchetto del genere dalla lista, ricompilate la lista con 'Ricarica la lista'.

La finestra dei pacchetti

Come abbiamo già detto, a destra, nella finestra dei pacchetti, vengono elencati i singoli pacchetti. Il contenuto di questa lista viene determinato dal filtro attualmente selezionato. Ad esempio, il filtro 'Selezione' vi mostra, nella finestra sulla destra, tutti i pacchetti della selezione attuale.

Nel package manager, ogni pacchetto ha uno stato che determina cosa debba avvenire con il pacchetto (ad esempio "Installare" o "Disinstallare" ecc.). Lo stato di un pacchetto, come per i filtri di selezione, viene rappresentato da un simbolo. Cliccando sul simbolo o aprendo il menu di contesto del pacchetto, potete passare da uno stato all'altro. Gli stati possibili sono numerosi e dipendono anche dalla situazione nel suo complesso: ad esempio, un pacchetto che non sia stato ancora installato non potrà essere selezionato per essere disinstallato. Troverete una lista degli stati e dei simboli nel menu 'Aiuto' → 'Simboli'.

Gli stati dei pacchetti nel package manager:

Non installare Questo pacchetto non è installato e non verrà installato.

Installare Questo pacchetto non è installato ma verrà installato.

Mantieni Questo pacchetto è già installato e rimane invariato.

Attualizza Questo pacchetto è già installato e verrà sostituito dalla nuova versione contenuta sul mezzo di installazione.

Elimina Questo pacchetto è già installato, ma verrà eliminato.

Escluso: non installare mai Questo pacchetto non è installato e non può venire installato in alcun caso. Viene trattato come se non esistesse. Se un pacchetto venisse selezionato automaticamente per risolvere una dipendenza, l'opzione "Escluso" ne impedisce l'installazione. Tuttavia, possono verificarsi delle incoerenze da risolvere manualmente ("verifica della consistenza"). "Escluso" è, pertanto, un'opzione per esperti.

Protetto Questo pacchetto è già installato e non viene modificato, dal momento che potrebbero sorgere dei problemi dovuti a dipendenze o conflitti con altri pacchetti. I pacchetti di terzi (ovvero i pacchetti che non portano la firma di SUSE) ricevono automaticamente questo stato, in modo che non vengano sovrascritte da versioni più recenti presenti sui mezzi di installazione. E' una funzione che può causare conflitti da risolvere manualmente.

Installare automaticamente Questo pacchetto è stato selezionato automaticamente dal package manager, perché necessario ad un altro pacchetto (risoluzione di dipendenze tra pacchetti). Per deselezionare un pacchetto simile, vi toccherà probabilmente usare la funzione "Escluso".

Attualizza automaticamente Questo pacchetto è già installato. Tuttavia, poiché vi è un altro pacchetto che richiede una versione aggiornata del medesimo, la versione del pacchetto installato verrà attualizzata automaticamente.

Elimina automaticamente Questo pacchetto è già installato, ma, a causa di un conflitto, deve essere eliminato, ad esempio quando si sostituisce il pacchetto in questione con un altro pacchetto.

Installa automaticamente (dopo la selezione)
Questo pacchetto è stato selezionato automaticamente per essere installato, perché parte di una selezione predefinita (ad esempio "Multimedia", "Sviluppo", ecc.).

Attualizza automaticamente (dopo la selezione)
Questo pacchetto è già installato, ma il mezzo di installazione contiene una versione più recente. Il pacchetto fa parte di una selezione predefinita (ad esempio "Multimedia" o "Sviluppo", ecc.) che volete aggiornare e quindi verrà attualizzato automaticamente.

Elimina automaticamente (dopo la selezione)
Questo pacchetto è già installato, ma una selezione predefinita ne richiede la cancellazione (ad esempio "Multimedia", o "Sviluppo", ecc.). Succede di rado.

Potete anche decidere se i sorgenti debbano essere installati assieme al pacchetto o meno. Questa informazione completa lo stato attuale del pacchetto, e pertanto non può essere modificata né tramite la casella di stato né tramite il menu di contesto. Avete invece alla fine della riga del pacchetto una casella per selezionare i sorgenti; troverete questa opzione anche nel menu 'Pacchetto'.

Installare i sorgenti Il codice sorgente viene installato insieme al pacchetto.

Non installare il codice sorgente I sorgenti non verranno installati.

Anche il colore dei nomi dei pacchetti dà delle indicazioni. I pacchetti già installati per i quali vi è disponibile una versione più recente vengono visualizzati in blu. I pacchetti installati che sono più recenti di quelli sul mezzo di installazione

assumono il color rosso. Dal momento che, a volte, le versioni non sono numerate in modo crescente, questa informazione può anche essere incorretta, ma potrà essere utile a rilevare pacchetti problematici. Se intende controllare il numero esatto della versione, fatelo servendovi della finestra di informazione.

La finestra d'informazione

La finestra di informazione si trova in basso a destra e presenta diverse schede che contengono delle informazioni sui pacchetti selezionati. La descrizione dei pacchetti selezionati è abilitata automaticamente. Cliccando sulle guide potete passare dalla scheda tecnica alla lista delle dipendenze ed ai dati riguardanti la versione.

La finestra delle risorse

In fase di selezione del software la finestra delle risorse in basso a sinistra vi informa sulla quantità di risorse necessarie per tutti i file system montati. Con ogni selezione cresce l'istogramma a colori. Finché prevale il verde vi è spazio a sufficienza. Col decresce della disponibilità di spazio l'istogramma assume sempre più una tinta rossa. Se selezionate un numero troppo elevato di pacchetti verrà visualizzato un messaggio di allerta.

La barra dei menu

La barra dei menu (in alto a sinistra) contiene tutte le funzioni che abbiamo appena descritto ed offre, a sua volta, quattro menu:

File Selezionate 'File' → 'Esporta' per salvare una lista di tutti i pacchetti installati in un file di testo. Questo file vi servirà, ad esempio, per ricostruire l'installazione su di un altro sistema o in un secondo momento. Questo file si lascia importare tramite l'opzione 'Importa' riproducendo l'identica selezione dei pacchetti salvati. In entrambi i casi, indicate la locazione del file o accettate la proposta del sistema.

Con 'Exit—scarta le modifiche', uscite dal package manager senza salvare le modifiche apportate alla selezione dei pacchetti. Per chiudere il modulo salvando le modifiche, cliccate su 'Quit— salva le modifiche'.

Pacchetto Le opzioni del menu 'Pacchetto' si riferiscono sempre al pacchetto attualmente selezionato nella finestra dei pacchetti. Anche se vengono visualizzati tutti gli stati possibili per un pacchetto potete selezionare tuttavia

solo gli stati che possono essere applicati al pacchetto. Tramite le caselle da spuntare (ingl. check box) potete determinare se installare il sorgente di un pacchetto o meno. L'opzione 'Tutti in questa lista' apre un sottomenu con gli stati di tutti i pacchetti della lista.

Altro Il menu 'Altro' vi offre delle soluzioni per la risoluzione delle dipendenze e dei conflitti tra pacchetti. Se avete già selezionato manualmente dei pacchetti per l'installazione, l'opzione 'Mostra le modifiche automatiche dei pacchetti' vi offre una lista di pacchetti selezionati automaticamente dal package manager per risolvere le dipendenze. Se a questo punto vi sono ancora dei conflitti irrisolti, il programma vi propone delle soluzioni.

Se decidete di reagire ai conflitti con "Ignora", tale impostazione viene salvata in modo permanente. Questo vi evita di dovere selezionare questa opzione ogni volta che aprite il package manager. Per disattivare questa funzione, cliccate su 'Ripristina conflitti di dipendenza ignorati'.

Aiuto Tramite 'Aiuto' → 'Rassegna' ottenete una breve spiegazione delle funzioni del package manager. Per sapere di più sui diversi stati di un pacchetto e dei relativi simboli, cliccate su 'Simboli'. Se preferite usare la tastiera, al posto del mouse, troverete illustrate tutte le abbrevazioni di tastiera sotto 'Tasti'.

Verifica della consistenza

Sotto la finestra d'informazione trovate il pulsante 'Controlla dipendenze' e la casella 'Controllo automatico'. Cliccando su 'Controlla dipendenze', il package manager verifica la presenza di eventuali conflitti o dipendenze irrisolte nei pacchetti da installare. In tal caso, il package manager seleziona automaticamente i pacchetti necessari alla risoluzione. Nel caso di conflitti, il package manager apre una finestra nella quale vengono elencati i conflitti e indicati vari modi di risolvere il problema.

Se attivate la 'Verifica automatica', ogni volta che viene modificato lo stato di un pacchetto verrà eseguita anche questa verifica. Questa funzione è molto utile, perché tiene sott'occhio la composizione dei pacchetti, ma richiede parecchia memoria e rallenta il funzionamento del package manager. Per questo motivo, è meglio non abilitare questa funzionalità all'avvio del package manager. Comunque, sta a voi decidere cosa fa al caso vostro: la verifica viene eseguita comunque, ogni volta che confermate la vostra selezione con 'Accetta'.

Nell'esempio riportato di seguito, `sendmail` e `postfix` non possono essere installati contemporaneamente. La figura 2.3 nella pagina successiva vi mostra

la presenza di un conflitto e vi invita a prendere una decisione. `postfix` è già installato, il che vuol dire che potete rinunciare all'installazione di `sendmail`, eliminare `postfix` o correre il rischio ed ignorare il conflitto.

Avvertimento

Risoluzione dei conflitti di pacchetti

Seguite in tal caso le proposte del package manager di YaST ne va la stabilità ed il buon funzionamento del vostro sistema.

Avvertimento

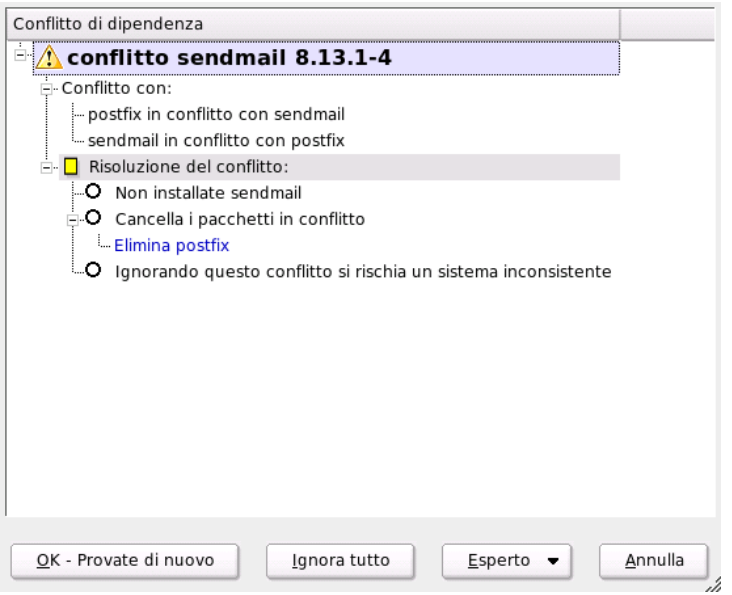

Figura 2.3: *La gestione dei conflitti del package manager*

2.2.2 Cambiare origine di installazione

YaST è in grado di gestire tutta una serie di origini di installazione e vi permette di selezionare quella più adatta alle vostre esigenze, cioè in base a se dovete eseguire un' installazione o un aggiornamento.

Dopo l'avvio del modulo viene mostrato un elenco delle origini di installazione disponibili. Se avete eseguito l'installazione dal CD, troverete solo il CD di installazione: cliccando su 'Aggiungi' potete aggiungere delle altre origini di installazione oltre al CD e DVD, come ad esempio un server NFS o FTP o addirittura delle directory sul disco rigido locale (si vedano i testi di aiuto di YaST per maggiori dettagli).

Le vari origini di installazione della lista sono corredate da un'indicazione di stato (nella prima colonna): potete 'abilitare o disabilitare' le origini indicate. Quando installate dei pacchetti di software o eseguite un aggiornamento, YaST sceglie tra le origini abilitate quella appropriata. Non appena uscite dal modulo con 'Chiudi', le vostre impostazioni verranno salvate ed applicate ai moduli di configurazione 'Installa e elimina software' o 'Aggiornamento del sistema'.

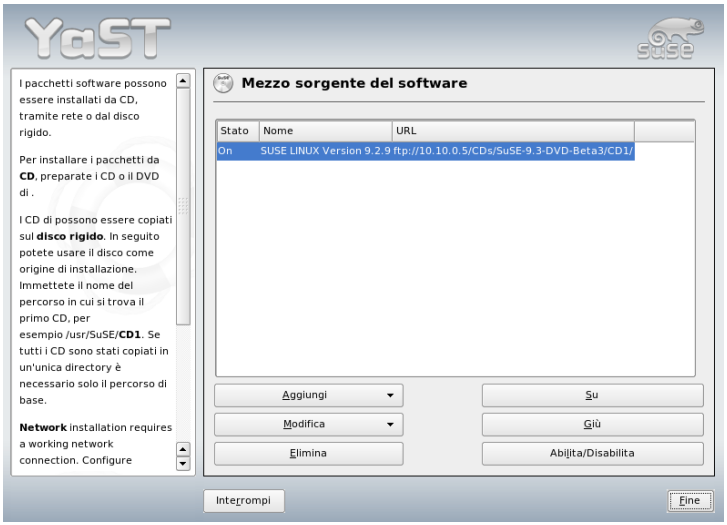

Figura 2.4: *Cambiare origine di installazione*

2.2.3 Aggiornamento in linea con YaST

YaST Online Update (YOU) vi permette di installare aggiornamenti e migliorie rilevanti. Sul server FTP di SUSE e diversi server mirror troverete le patch da scaricare.

Tramite ‘Origine di installazione’ potete selezionare il server che fa al vostro caso. Selezionando un server, l’URL viene copiata nel campo inferiore dove potrete editarla. Potete anche indicare URL locali che si seguono questa sintassi `file:/mio/percorso` o anche solo `/mio/percorso`. L’elenco può essere ampliato tramite ‘Nuovo server’. Tramite ‘Modifica server’ si lasciano modificare le impostazioni del server selezionato.

All’avvio del modulo è abilitata l’opzione ‘Selezione manuale delle patch’ che permette di scaricare solo determinate patch. Per scaricare tutti i pacchetti di aggiornamento disponibili, disabilitate questa opzione. Tenete presente che quest’ultima selezione può richiedere molto tempo a seconda della larghezza di banda e volume di dati da trasmettere.

Se attivate la casella ‘Scaricare nuovamente tutte le patch’ verranno scaricate tutte le patch, i pacchetti e la manualistica. Altrimenti, verranno scaricate di default solo le patch non ancora installate.

Sussiste anche la possibilità di impostare il programma in modo che sia lui ad occuparsi automaticamente di tenere aggiornato il sistema. Con ‘Configura update automatico’, potete configurare un processo che vada a cercare ad intervalli regolari nuovi update e li installi, del tutto automaticamente. Naturalmente, per il sistema in questione dovrà essere data la possibilità di collegarsi al server all’ora prestabilita.

Per eseguire l’aggiornamento, cliccate su ‘Prossimo’. Durante la procedura d’aggiornamento manuale verrà generata una lista delle patch disponibili. Dopodiché, viene avviato il package manager (si veda la sezione 2.2.1 a pagina 40. Il package manager, ovvero gestore dei pacchetti offre un filtro per le patch YOU, di modo che a voi non resta che selezionare quelle che desiderate installare. Alcune saranno già selezionate perché particolarmente utili al sistema. Di solito si consiglia di accettare le proposte.

Dopo aver fatto la vostra selezione, cliccate su ‘Accetto’ e tutti gli update selezionati verranno scaricati dal server ed installati nel sistema. La durata di questi due processi dipende dalla qualità della connessione e dalle capacità del computer. Ogni problema vi verrà comunicato in una finestra a parte, in modo che possiate eventualmente saltare il pacchetto causa di difficoltà. Alcune patch, prima dell’installazione, visualizzano una finestra con dei dettagli tecnici.

Potete seguire il processo attraverso una finestra protocollo. Alla fine dell’installazione, uscite da YOU con ‘Fine’. Se dopo l’installazione i file aggiornati non dovessero servirvi più, potrete cancellarli con ‘Elimina pacchetti sorgente dopo l’update’. Dopodiché, il programma esegue SuSEconfig per adeguare la configurazione del sistema.

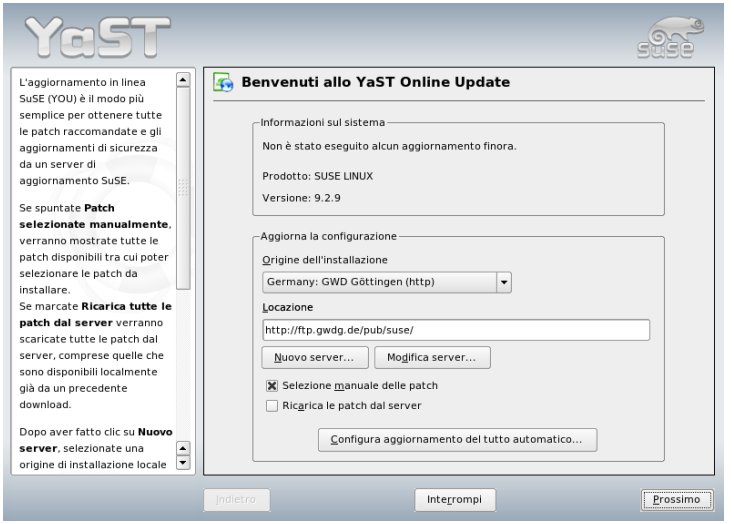

Figura 2.5: *YaST Online Update*

2.2.4 Update dal CD delle patch

In questo caso, contrariamente all'aggiornamento in linea (online update), le patch non vengono scaricate dal server ftp, ma installate dal CD. Il vantaggio che ne deriva è un aggiornamento considerevolmente più veloce. Inserendo il CD delle patch, vengono mostrate tutte le patch contenute sul CD. A questo punto potete scegliere quelle da installare. Il modulo emette un messaggio di errore se non è stato inserito alcun CD delle patch. Inseritelo nell'apposito lettore e riavviate il modulo.

2.2.5 Aggiornamento del sistema

Questo modulo vi permette di attualizzare la versione del vostro sistema. Con il sistema in esecuzione è comunque possibile aggiornare solo applicazioni, non però il sistema di base di SUSE LINUX. Per fare ciò è necessario eseguire il boot dal mezzo di installazione (ad es. CD). Nel dialogo di selezione del modo di installazione di YaST, scegliete 'Aggiornamento del sistema esistente' al posto di 'Nuova installazione'.

La procedura da seguire durante l'aggiornamento ricorda quella dell'installazione: YaST inizia con l'analisi lo stato del sistema, propone un'appropriata strategia di aggiornamento e presenta quindi il risultato in una finestra di proposta. Alcuni punti, come 'Lingua' e 'Mappatura della tastiera', vengono trattati nella sezione dedicata alla procedura di installazione (si veda la sezione 1.3 a pagina 8). Nelle pagine seguenti, pertanto ci concentreremo sulle impostazioni che riguardano da vicino l'update.

Selezionato per l'aggiornamento

Se sul vostro sistema avete installato diverse versioni di SUSE LINUX, potete scegliere qui la partizione da usare per l'update.

Opzioni di aggiornamento

In questo dialogo, impostate il modo in cui il vostro sistema debba essere aggiornato. Le possibilità sono due.

Aggiornamento con l'installazione di nuovo software
: Se desiderate aggiornare il vostro sistema per intero, selezionate una delle selezioni predefinite. Queste selezioni sono le stesse che vi vengono proposte durante il procedimento di installazione e assicurano che vengano installati anche pacchetti finora non inclusi.

Attualizzare solo pacchetti installati Con questa opzione, il programma aggiorna solo i pacchetti già presenti sul sistema, senza aggiungerne alcuno.

Con 'Elimina pacchetti obsoleti', potete anche decidere di cancellare i pacchetti che non sono più inclusi nella nuova versione. Questa opzione è preimpostata, per evitare lo spreco di risorse del sistema per pacchetti obsoleti.

Pacchetti

Con 'Pacchetti', avviate il package manager e potete selezionare o deselezionare in modo mirato dei pacchetti. Eseguite il controllo di consistenza per risolvere conflitti di pacchetti rilevati. Il funzionamento del package manager viene spiegato nella sezione 2.2.1 a pagina 40.

Backup

Durante un update vengono aggiornati anche i file di configurazione dei pacchetti. Visto che non si può escludere che vengano apportate delle modifiche a file del genere nel vostro sistema attuale, di solito si consiglia di eseguire una copia di sicurezza dei file da aggiornare o da sostituire. In questo dialogo potete determinare l'estensione della copia di sicurezza.

Importante

Estensione del back-up

Tenete presente che questo backup non interessa il software ma solo i file di configurazione.

Importante

Importanti indicazioni sull'update

Dal punto di vista del software, l'aggiornamento del sistema è un processo molto complesso. Per ogni pacchetto, YaST deve verificare quale versione si trovi nel sistema e cosa fare per sostituire correttamente la vecchia versione con quella nuova. In particolare, YaST tenterà di passare alla nuova versione le impostazioni personali dell'utente, in modo che non si debba rifare tutta la configurazione. Può verificarsi il caso che dopo un update determinate impostazioni siano incompatibili con la nuova versione dell'applicazione.

Un update diventa problematico quando si tratta di aggiornare una versione molto vecchia e/o la configurazione dei pacchetti non segue lo standard. Può verificarsi il caso che la vecchia configurazione non potrà essere assunta per intero, allora si consiglia di eseguire una nuova configurazione. Prima di eseguire un update si consiglia sempre di fare un back-up della configurazione esistente.

2.2.6 Verifica del mezzo di installazione

Se doveste incontrare delle difficoltà con il mezzo di installazione di SUSE LINUX grazie a questo modulo potete eseguire una verifica dei CD o DVD. In casi rari alcuni dispositivi non riescono a leggere correttamente dei CD o DVD. E' una problematica che interessa in prima linea mezzi "fatti da sé". Per eseguire comunque una verifica dei CD o DVD di SUSE LINUX, inseriteli nel lettore e lanciate questo modulo. Cliccate su 'Avvia' e YaST verifica la somma di controllo MD5 dei CD o DVD. Questo processo può durare un pò e se vengono rilevati degli errori, non utilizzare questo mezzo ai fini dell'installazione.

2.3 Hardware

Il nuovo hardware deve essere integrato o connesso nel modo prescritto dal costruttore. Accendete dispositivi esterni come stampante o modem e lanciate il relativo modulo di YaST. La maggior parte dell'hardware in commercio viene riconosciuta automaticamente da YaST, che ne mostra le specificazioni tecniche. Se il rilevamento automatico non dovesse funzionare, YaST vi offre una lista di modelli o produttori tra cui poter selezionare il vostro dispositivo. Consultate anche la documentazione dell'hardware, se i dati riportati sul dispositivo stesso non dovessero bastare.

Importante

Designazioni di modello

Fate attenzione: se il vostro modello non figura nella lista, sceglietene uno con una denominazione simile. A volte, però, bisogna essere precisi, dal momento che denominazioni simili non sono una garanzia di compatibilità.

Importante

2.3.1 I lettori CD-Rom e DVD

Durante l'installazione, tutti i lettori di CD-Rom vengono integrati nel sistema. Questo significa che vengono inclusi nel file `/etc/fstab` e create le rispettive sottodirectory sotto `/media`. Con questo modulo di YaST, potete integrare successivamente degli altri lettori.

All'avvio del modulo vedete una lista dei lettori rilevati. Cliccate sulla casella del vostro nuovo lettore e terminate il procedimento di integrazione nel vostro sistema cliccando su 'Fine'.

2.3.2 Stampante

Per delle informazioni dettagliate in tema di processo di stampa sotto Linux rimandiamo al capitolo 12 a pagina 249 che tratta in via generale le questioni inerenti a questa tematica. YaST configura la stampante in modo automatico o assiste l' utente durante il procedimento di configurazione manuale della stampante. Una volta conclusa tale fase l'utente potrà stampare dalla linea di comando o

configurare delle applicazioni in modo da poter utilizzare il sistema di stampa. Una descrizione dettagliata del modo di configurare delle stampanti con YaST è reperibile nella sezione 12.5.1 a pagina 254.

2.3.3 Hard disk controller

Di solito YaST configura l'hard disk controller del vostro sistema durante l'installazione. Per installarne degli altri potete ricorrere nuovamente a questo modulo di YaST. Tramite questo modulo potete anche modificare la configurazione del controller, cosa normalmente non necessaria.

Questa finestra contiene una lista degli hard disk controller rilevati e permette di attribuirvi un modulo del kernel adeguato con parametri specifici. Cliccate ora su 'Verifica caricamento del modulo' per verificare se i parametri impostati funzionino, prima di memorizzarli in modo permanente nel sistema.

Avvertimento

Configurazione del controller del disco rigido

Si tratta di un modulo per esperti: fatene uso accorto ed informato. Delle impostazioni errate in questo modulo potrebbero rendere il sistema non più avviabile. Vi consigliamo sempre e comunque di eseguire un test.

Avvertimento

2.3.4 Informazioni sull'hardware

Prima di poter iniziare il procedimento di configurazione dei componenti hardware, YaST esegue il rilevamento dell'hardware. I dati che raccoglie vengono riportati in questo dialogo, i quali sono particolarmente utili quando volete inviare una richiesta al servizio di supporto contente dei dati inerenti al vostro hardware.

2.3.5 Modo IDE DMA

Questo modulo vi permette di attivare o disattivare il cosiddetto modo DMA per i dischi rigidi ed i lettori CD/DVD di tipo IDE, dopo l'installazione del sistema. Questo modulo non funziona con hardware SCSI. I modi DMA possono aumentare sensibilmente le prestazioni, ovvero la velocità di trasmissione dei dati, del vostro sistema.

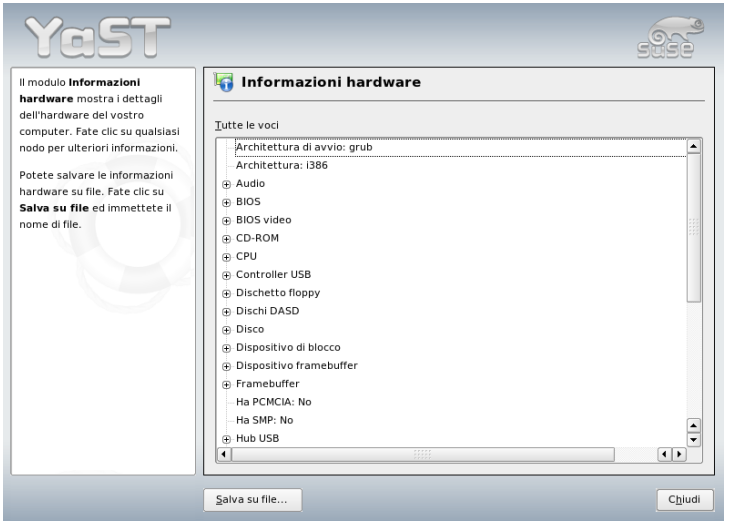

Figura 2.6: *Visualizza informazioni hardware*

Durante l'installazione del sistema, il kernel di SUSE LINUX attiva automaticamente il DMA per il disco rigido ma non per il lettore CD, dal momento che con questi dispositivi si sono verificati spesso dei problemi. Tramite il modulo DMA potete attivare il DMA per i vostri dispositivi. Se il lettore supporta il modo DMA correttamente, attivandolo incrementerete il tasso di trasmissione.

Importante

DMA sta per direct memory access che potremmo tradurre con accesso diretto alla memoria, sarebbe a dire che i dispositivi potranno inviare i dati direttamente alla RAM, senza dover passare per il processore.

Importante

2.3.6 Scanner

Connettete e accendete lo scanner: il modulo di YaST - una volta lanciato - dovrebbe rilevarlo automaticamente. In questo caso, appare il dialogo di installazione dello scanner. In caso contrario, procedete con la configurazione manu-

ale. Se ne avete già installati diversi, verrà visualizzato un elenco degli scanner già configurati che potrete modificare o eliminare. Per aggiungerne uno nuovo, cliccate su 'Aggiungi'.

Ora, viene eseguita un'installazione con parametri standard. YaST vi comunica quando l'installazione è conclusa. Per testare lo scanner, inseritevi un qualche tipo di immagine e cliccate su 'Test'.

Scanner non rilevato

Solo gli scanner supportati vengono riconosciuti in modo automatico. Quelli che sono connessi ad un altro host della rete, non vengono rilevati. Ai fini della configurazione manuale si distinguono tre tipi di scanner: scanner USB, SCSI o di rete.

Scanner USB Inserite il produttore e modello. YaST tenterà di caricare i moduli USB appropriati. Se si tratta di uno scanner molto recente, può darsi che i moduli non vengano caricati automaticamente. In questo caso, verrà visualizzata una finestra in cui poter caricare il modulo USB manualmente; per maggiori indicazioni consultate i testi illustrativi di YaST.

Scanner SCSI Indicate il tipo di dispositivo (ad es.: `/dev/sg0`). Attenzione: uno scanner SCSI non può essere connesso con il sistema in esecuzione. Spegnete prima il sistema.

Scanner di rete Qui sono richiesti il nome host o l'indirizzo IP. Consultate l'articolo della banca dati di supporto sulla configurazione di uno scanner di rete: *Scanning in Linux* (`http://portal.suse.com/sdb/en/index.html`, parola chiave *scanner*).

Se il vostro scanner non è stato rilevato, probabilmente non viene supportato. A volte, però, anche gli scanner compatibili non vengono riconosciuti. In questo caso, selezionate manualmente lo scanner nell'apposito elenco dei produttori e modelli. Se il vostro modello non è incluso nell'elenco, cliccate su 'Interrompi'. Tutti gli scanner compatibili con Linux sono riportati all'indirizzo `http://cdb.suse.de/` e `http://www.mostang.com/sane`.

Avvertimento

Selezione manuale di uno scanner

La configurazione manuale di uno scanner va fatta con cognizione di causa, perché una selezione errata potrebbe danneggiare il vostro hardware.

Avvertimento

Problemi con il rilevamento dello scanner

Se il vostro scanner non è stato rilevato, può darsi che:

- Lo scanner non venga supportato. Tutti gli scanner compatibili con Linux sono elencati al sito `http://cdb.suse.de/`
- Il controller SCSI non sia stato installato correttamente.
- Ci siano problemi di terminazione con la porta SCSI.
- Il vostro cavo SCSI sia troppo lungo.
- Lo scanner abbia un "SCSI light controller" che non è compatibile con Linux.
- Lo scanner sia difettoso.

Avvertimento

Uno scanner SCSI non va connesso o disconnesso con il sistema in esecuzione. Spegnete prima il sistema.

Avvertimento

Per maggiori dettagli, consultate il capitolo dedicato a `kooka` nel *Manuale dell'utente*.

2.3.7 Audio

Quando lanciate il modulo di configurazione dell'audio, YaST prova a rilevare automaticamente la scheda audio. Potete configurare una o più schede audio: configuratele selezionandole una alla volta. Il pulsante 'Configura' vi porta al menu 'Setup'. Il pulsante 'Modifica', invece, vi consente di cambiare i

parametri delle schede già configurate. Con 'Fine' salvate le vostre impostazioni e concludete la configurazione della scheda'audio.

Se YaST non riconosce la vostra scheda automaticamente, andate al menù 'Configurazione suono', cliccate su 'Aggiungi scheda sonora' per entrare nella finestra in cui selezionare una scheda sonora ed il relativo modulo. Per il reperimento dati richiesti fate riferimento alla documentazione della vostra scheda audio. Un elenco delle schede sonore e rispettivi moduli sonori supportati da ALSA lo trovate sotto `/usr/share/doc/packages/alsa/cards.txt` e all'url `http://www.alsa-project.org/~goemon/`. Dopo aver fatto le vostre selezioni, cliccate su 'Prossimo' per tornare a 'Setup'.

Setup

Il 'Setup automatico veloce' configura la scheda senza porre delle domande o dover fare delle selezioni e senza che venga eseguito alcun test. Il 'Setup normale', invece, vi porta al menu 'Volume della scheda audio', dove potrete regolare il volume in uscita e testare la scheda. Nel 'Setup esteso' potete modificare manualmente le opzioni della scheda sonora.

Qui potete configurare inoltre il joystick, cliccando sulla corrispondente casella. Appare un dialogo con diversi tipi di joystick. Selezionate il tipo di joystick e cliccate quindi su 'Prossimo'.

Volume della scheda audio

Questa schermata vi permette di eseguire un test della vostra configurazione audio. Tramite i pulsanti '+' e '-' potete intervenire sul volume. Per non danneggiare né gli altoparlanti né il vostro udito iniziate con un valore di circa 10%. Cliccate su 'Test' e dovreste sentire un suono prova. In caso contrario, alzate il volume. Per concludere la configurazione e salvare i parametri, cliccate su 'Prossimo'.

La configurazione dell'audio

L'opzione 'Elimina' vi permette di disinstallare una scheda. Le schede già configurate vengono disattivate nel file `/etc/modprobe.d/sound`. Cliccando su 'Opzioni' entrate una finestra dialogo in cui poter personalizzare le opzioni dei moduli audio manualmente. L'opzione 'Aggiungi scheda audio' vi permette di integrare altre schede. Se YaST rileva automaticamente un'altra scheda, giungete al menu 'Configurare una scheda audio'; altrimenti giungete alla 'Selezione manuale della scheda audio'.

Con una scheda audio `Creative Soundblaster Live` o una `AWE` potete usufruire dell'opzione 'Installa sound font' e copiare automaticamente i sound

font SF2 dal CD-Rom originale del driver Soundblaster sul vostro disco rigido. I sound font vengono salvati nella directory `/usr/share/sfbank/creative/`.

Per la riproduzione di file MIDI dovreste abilitare la check box 'Avvia sequenziatore'. In questo modo, con i moduli audio vengono caricati anche i moduli necessari per il supporto del sequenziatore.

Cliccate su 'Fine' e vengono salvati volume e configurazione di tutte le schede installate. I parametri del miscelatore vengono salvati nel file `/etc/asound.conf` mentre i file di configurazione di ALSA si aggiungono al file `/etc/modprobe.conf`.

2.3.8 Le schede TV e radio

Una volta avviato il modulo di YaST, appare il dialogo 'Configura schede TV e radio'. Se la scheda viene riconosciuta automaticamente, verrà riportata nella lista. Cliccate sulla scheda e poi su 'Configura'. Se la scheda non è stata riconosciuta, selezionate 'Altre (non riconosciute)'. Cliccate su 'Configura' per proseguire con la selezione manuale della vostra scheda dall'elenco dei produttori e modelli.

Se avete già delle schede TV o radio configurate, potete modificarne i parametri con 'Modifica'. Si aprirà il dialogo 'Elenco di schede TV e radio', con tutte le schede del sistema. Selezionatene una e cambiatene la configurazione con 'Modifica'.

Durante il rilevamento automatico della scheda, YaST tenta di attribuirle un sintonizzatore. Se non siete sicuri lasciate i parametri su 'Standard (riconosciute)' e verificatene il corretto funzionamento. Se non riuscite a sintonizzare tutti i canali, forse il rilevamento automatico del sintonizzatore non ha funzionato. In questo caso, cliccate sul pulsante 'Seleziona sintonizzatore' e selezionate quello appropriato dalla lista.

Se avete dimestichezza con questo tipo di scheda potete proseguire con il dialogo per esperti e configurare lì la scheda radio o TV. Potrete selezionare anche il modulo del kernel ed i suoi parametri, nonché verificare i parametri del driver della scheda TV. Potrete selezionare un parametro e assegnargli un nuovo valore nell'apposito rigo. Con 'Applica', i nuovi valori vengono salvati, mentre con 'Ripristina' ripristinate quelli preimpostati.

Nel dialogo 'Scheda TV e radio, audio', potete connettere la scheda TV o radio alla scheda audio installata. In questo caso bisognerà configurare entrambe le schede e collegare l'uscita della scheda TV o radio con l'ingresso audio esterno della scheda sonora tramite un cavo speciale. La scheda audio deve essere già

installata e l'ingresso esterno attivato. In caso contrario, cliccate su 'Configura scheda audio' e provvedete (si veda la sezione 2.3.7 a pagina 58.

Se la vostra scheda TV o radio offre anche delle uscite per altoparlanti, approfittatene: vi risparmiate la configurazione della scheda audio. In commercio troverete anche delle schede TV senza funzionalità audio (ad esempio, quelle per le telecamere CCD) che non necessitano questo tipo di configurazione.

2.4 Dispositivi di rete

Il gruppo modulo 'Dispositivi di rete' vi permette di rilevare e configurare questi dispositivi. La sezione 22.4 a pagina 415 vi offre una descrizione particolareggiata del processo di configurazione delle schede di rete con YaST fornendo delle utili indicazioni sul modo di creare delle reti. La configurazione di dispositivi wireless viene illustrata nel capitolo 17 a pagina 333.

2.5 Servizi di rete

Questo gruppo contiene in prima linea gli strumenti richiesti per configurare i vari tipi di servizi di una rete come la risoluzione dei nomi, l'autenticazione degli utenti e server di file.

2.5.1 Mail Transfer Agent

Questo modulo vi permette di eseguire tutte le impostazioni richieste per poter spedire le vostre e-mail tramite sendmail, postfix o il server SMTP del vostro provider. Per scaricare delle e-mail potete usare il programma fetchmail, per il quale potete inserire di dati del server POP3 o IMAP del vostro provider. Alternativamente, tramite un qualsiasi programma di posta elettronica, come ad esempio KMail o Evolution potete configurare come al solito i dati di accesso POP ed SMTP, ovvero usare POP3 per la posta in entrata e SMTP per quella in uscita. In tal caso, questo modulo non vi serve.

Se preferite servirvi di YaST per la configurazione della vostra posta elettronica specificate il tipo di connessione ad Internet nel primo dialogo del modulo di configurazione. Ecco le opzioni a vostra disposizione:

'Permanente' Se siete connessi in modo permanente a Internet selezionate questa opzione. Il vostro computer è interrottamente connesso e quindi non sarà necessario connettersi appositamente. Scegliete questa opzione anche se il vostro computer fa parte di una rete locale con un server di posta centrale per accedere in qualsiasi momento alle vostre e-mail.

'Connessione' Questo punto riguarda tutti gli utenti che a casa hanno un computer che non fa parte di una rete e che si connettono saltuariamente ad Internet.

Nessuna connessione Se non avete accesso all'Internet e non fate parte di una rete e, di conseguenza, non potete né mandare né ricevere della posta elettronica.

Un'altra opzione utile è la possibilità di abilitare il programma antivirus AMaViS. Questo pacchetto viene automaticamente installato non appena avrete attivato la funzione di filtraggio delle mail. Nei dialoghi che seguono, impostate il server di posta per le e-mail in uscita (di solito il server SMTP del vostro provider) ed i parametri della posta in entrata. Se usate una connessione di tipo "dial-up", potete anche impostare diversi server POP o IMAP per la posta in entrata di diversi utenti. Infine, questo dialogo vi permette di assegnare gli alias, di impostare il mascheramento o i domini virtuali. Per uscire dal dialogo di configurazione della posta elettronica, premete su 'Fine'.

2.5.2 Ulteriori servizi disponibili

YaST offre inoltre tutta una serie di moduli di rete.

Server DHCP YaST vi permette di impostare in modo semplice un proprio server DHCP. Nel capitolo 27 a pagina 479 vengono illustrati i concetti di base di questa tematica e descritti i singoli passaggi per effettuare la configurazione con YaST.

Server DNS Nel caso di reti di maggior dimensione è consigliabile impostare un server DNS per la risoluzione dei nomi. Come eseguire la configurazione con YaST viene descritto nella sezione 24.1 a pagina 446. Il capitolo 24 a pagina 445 contiene maggiori dettagli in tema di DNS.

DNS e nome dell'host Con questo modulo potete configurare un nome host ed il DNS, se non avete già provveduto durante la configurazione dei dispositivi di rete. Potrete inoltre cambiare il nome dell'host e del dominio. Se

avete configurato correttamente l'accesso via DSL, modem o ISDN, questo dialogo conterrà una lista di server dei nomi presa direttamente dai dati del provider. Se fate parte di una rete locale, il vostro nome host vi è stato probabilmente assegnato via DHCP. In questo caso, non modificatelo!

Server HTTP Se intendete avere un proprio server web configurate Apache con l'aiuto di YaST. Per ulteriori informazioni rimandiamo al capitolo 30 a pagina 521.

Nomi degli host La risoluzione dei nomi degli host nel caso di piccole reti può avvenire al boot anche tramite questo modulo come alternativa a DNS. Le registrazioni di questo modulo riflettono i dati del file `/etc/hosts`. Per maggiori informazioni rimandiamo alla sezione /etc/hosts a pagina 432.

Client LDAP In tema di autenticazione degli utenti, LDAP rappresenta una alternativa a NIS. Per maggiori dettagli su LDAP nonché per una descrizione dettagliata del processo di configurazione di un client tramite YaST rimandiamo alla capitolo 29 a pagina 495.

Client NFS e server NFS NFS vi dà modo di gestire un file server sotto Linux al quale potranno accedere tutti i membri della rete. Un file server mette a disposizione determinati programmi e file ma anche dello spazio di memoria per gli utenti. Nel modulo 'Server NFS', impostate il vostro sistema come server NFS e stabilite quindi le directory da esportate, ovvero da mettere a disposizione degli utenti della rete. Ogni utente (che riceve il permesso) può montare queste directory nel proprio albero dei file. Per una descrizione del modulo YaST e degli approfondimenti in tema di NFS rimandiamo al capitolo 26 a pagina 473.

Client NIS e server NIS Non appena amministrate più di un sistema diventa improponibile eseguire localmente l'amministrazione degli utenti (tramite i file `/etc/passwd` e `/etc/shadow`). In questi casi si consiglia di amministrare i dati degli utenti centralmente su un server e di distribuirli da lì a tutti i client. Accanto a LDAP e Samba potete ricorre a NIS per assolvere un compito del genere. Per delle informazioni dettagliate su NIS e sulla configurazione con YaST rimandiamo a capitolo 25 a pagina 467.

NTP Client L'NTP (ingl. Network Time Protocol) è un protocollo per la sincronizzazione dell'ora dei client tramite la rete. Per maggiori dettagli su NTP e la descrizione del processo configurativo tramite YaST rimandiamo al capitolo 28 a pagina 489.

Servizi di rete (inetd) Questi tool vi permettono di impostare i servizi di rete, ad esempio finger, talk, ftp etc., da avviare al boot di SUSE LINUX. Questi servizi consentono ad host esterni di collegarsi al vostro sistema. Per ogni servizio potete impostare diversi parametri. Di default non viene avviato il servizio superiore che amministra i singoli servizi (ovvero inetd o xinetd).

Dopo l'avvio del modulo selezionate se lanciare inetd o xinetd. Il deamon selezionato può essere avviato con una selezione standard di servizi di rete oppure potete definire voi una serie di servizi tramite 'Aggiungi', 'Elimina' e 'Modifica'.

Avvertimento

Configurare servizi di rete (inetd)

La configurazione dei servizi di rete è un processo di una certa complessità che richiede delle nozioni approfondite per quel che riguarda il concetto che sta alla base dei servizi di rete Linux.

Avvertimento

Proxy Questo modulo vi consente di modificare le impostazioni proxy valide per tutto il vostro sistema. Per delle informazioni dettagliate in tema di Proxy rimandiamo al capitolo 33 a pagina 579.

Amministrazione da un host remoto Per poter amministrare il vostro sistema tramite una connessione VNC da un host remoto, dovete consentire la creazione di una connessione verso questo modulo di YaST. L'amministrazione ricorda la procedura di installazione illustrata nella sezione 3.2.2 a pagina 91.

Routing Questo strumento è richiesto se vi connettete ad Internet tramite un gateway di una rete locale. Per DSL l'indicazione del gateway serve solo alla corretta configurazione della scheda di rete, comunque si tratta solo di un valore di riempimento, detto anche dummy.

Configurazione di un server/client Samba
In una rete eterogenea composta da host Linux e Windows, Samba provvede alla realizzazione del processo comunicativo tra i due sistemi operativi. Per maggiori informazioni su Samba nonché sulla configurazione di client e server rimandiamo alla capitolo 32 a pagina 567.

2.6 Sicurezza e utenti

Una delle caratteristiche fondamentali di Linux è il fatto di essere un sistema multiutente: sullo stesso sistema possono lavorare più utenti contemporaneamente e del tutto autonomamente. Ognuno ha il suo user account, a cui potrà accedere indicando il proprio nome utente o login e password personale. Inoltre, ogni utente ha una propria directory home in cui risiedono tutti i file e le impostazioni dell'utente.

2.6.1 Amministrazione degli utenti

Lanciate questo modulo di configurazione e troverete una maschera per l'amministrazione degli utenti e dei gruppi. Se intendete eseguire delle modifiche riguardanti gli utenti, YaST vi fornirà una rassegna di tutti gli utenti locali del sistema. Se vi trovate all'interno di una rete di medio-grandi dimensioni tramite 'Stabilire filtro' potrete farvi elencare tutti gli utenti del sistema (ad esempio, `root`) o utenti NIS. Potete anche personalizzare i parametri dei filtri in modo da non dover passare da un gruppo all'altro potendoli combinare a piacimento. Per creare un nuovo utente, cliccate su 'Aggiungi' e riempite la maschera successiva. Alla fine della configurazione, l'utente potrà immettersi nel sistema con il suo nome di login e password. Tramite 'Dettagli' potete cesellare le impostazioni del profilo degli utenti. Potete impostare manualemente l'ID dell'utente, la directory home e la shell di login di default. Inoltre, potete aggiungere un nuovo utente ad un determinato gruppo. Per fissare la scadenza della password andate su 'Impostazioni password'. Tramite 'Modifica' potete modificare le impostazioni in qualsiasi momento. Per cancellare un utente, selezionatelo dalla lista e premete il pulsante 'Elimina'.

Per compiti di amministrazione di rete più avanzati, potete fissare i parametri standard necessari alla configurazione di nuovi utenti alla voce 'Opzioni per esperti ...', dove potete impostate il metodo di autenticazione (NIS, LDAP, Kerberos o Samba), come anche l'algoritmo della cifratura della password. Si tratta di impostazioni di sicuro interesse per grandi reti (aziendali).

2.6.2 Amministrazione dei gruppi

Avviate il modulo di amministrazione dei gruppi dal centro di controllo di YaST o cliccando sulla casella 'Gruppi' nel modulo di amministrazione dei gruppi. Entrambi i moduli offrono più o meno le stesse funzioni per creare, modificare o cancellare dei gruppi.

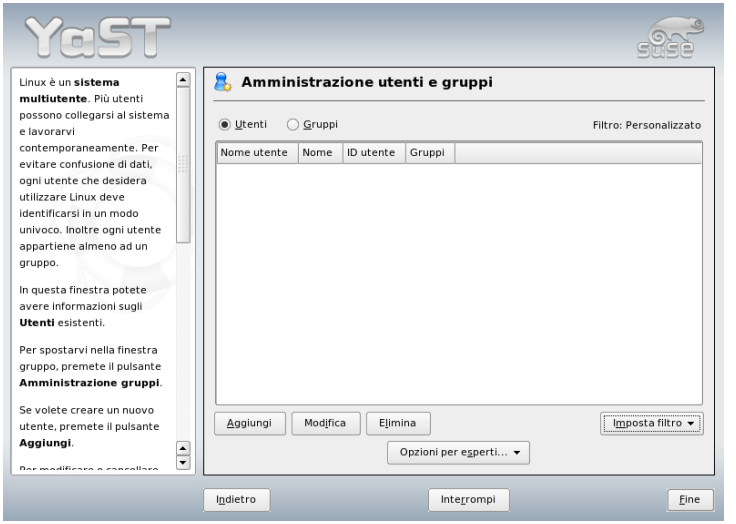

Figura 2.7: *Amministrazione degli utenti*

Per facilitarvi il compito di amministrazione degli utenti, YaST compone una lista di tutti i gruppi. Quindi, per eliminarne uno, basta selezionarlo nella lista (il gruppo viene evidenziato in blu scuro) e quindi cliccare su 'Elimina'. Le opzioni 'Aggiungi' e 'Modifica' richiedono il nome, l'ID di gruppo (gid) ed i membri del gruppo. Eventualmente, potrete anche impostare una password per accedere al gruppo selezionato. Questo dialogo è strutturato come quello per l' 'Amministrazione utenti'.

2.6.3 Impostazioni di sicurezza

Nella finestra iniziale 'Configurazione della sicurezza locale' troverete le seguenti quattro opzioni: 'Level 1' è per i sistemi a postazione unica (preconfigurato), 'Level 2' è per le postazioni di lavoro con rete (preconfigurato), 'Level 3' è per i server con rete (preconfigurato) e 'Personalizzato' permette all'utente di eseguire proprie impostazioni.

Selezionate un livello e verrà applicato il livello di sicurezza preconfigurato. In questo caso cliccate su 'Fine'. La voce 'Dettagli' vi dà accesso ad una serie

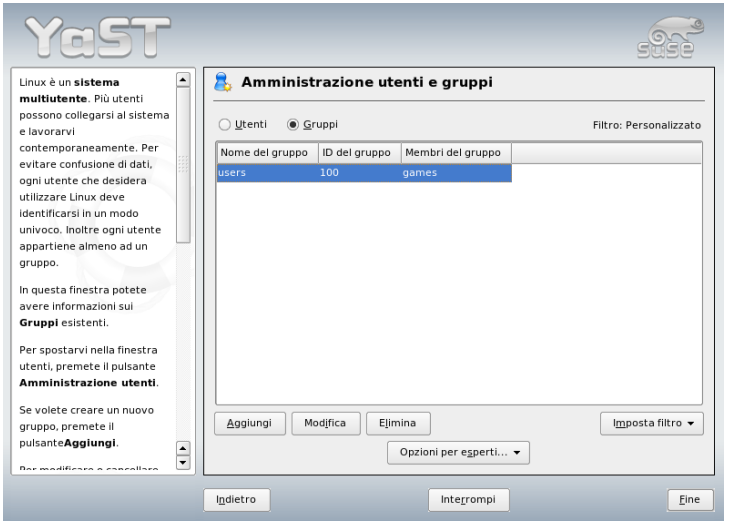

Figura 2.8: *Amministrazione dei gruppi*

di parametri. Selezionando 'Personalizzato', si passa automaticamente da un dialogo all'altro con 'Prossimo'. Qui troverete i valori preimpostati.

'L'impostazione della password' Se desiderate che le nuove password vengano controllate dal sistema, prima di essere attivate, cliccate sulle due caselle 'Controlla le nuove password' e 'Test di plausibilità delle password'. Fissate la lunghezza massima e minima delle password dei nuovi utenti. Poi, impostate la data di scadenza delle password e decidete quanti giorni prima della scadenza il sistema debba avvertire l'utente della scadenza stessa (con un messaggio sulla console di testo, al momento del login).

'Le impostazioni dell'avvio del sistema'
Come deve essere interpretata la combinazione di tasti Ctrl-Alt-Canc? Di solito, sulla console di testo, con questa combinazione di tasti si riavvia il sistema e non andrebbe modificata, fatta eccezione per il caso in cui il vostro sistema o il vostro server è accessibile a tutti e c'é da temere che a qualcuno venga la tentazione di eseguire questa azione senza il vostro permesso. Se selezionate 'Stop', la combinazione di tasti avrà come effetto lo spegnimen-

to del sistema. Selezionando invece 'Ignora', questa combinazione di tasti verrà ignorata.

Chi ha il permesso di spegnere il sistema da KDM (KDE-Display-Manager, il login grafico)? Specificatelo sotto 'Comportamento di spegnimento di KDM'. Sono a vostra disposizione le seguenti opzioni. 'Solo Root' (l'amministratore del sistema), 'Tutti gli utenti', 'Nessuno' o 'Utenti locali'. Se scegliete 'Nessuno', il sistema potrà essere spento solo dalla console di testo.

'Le impostazioni di login' Dopo un login fallito, bisogna aspettare di solito pochi secondi prima di poter riprovare. Questo intervallo favorisce la sicurezza delle password offrendo maggior protezione soprattutto in quei casi in cui qualcuno dovesse tentare di bucare la vostra password servendosi di programmi particolari detti sniffer. Inoltre sussiste la possibilità di 'Registrare i tentativi di login falliti' e di 'Registrare i tentativi di login riusciti'. Questa opzione vi permette di tenere sott'occhio i login consultando `/var/log` se sospettate che qualcuno stia cercando di compromettere la vostra password. Selezionando la casella 'Permetti login grafico da remoto', concederete ad altri utenti il permesso di accedere allo schermo di login grafico dalla rete. Questa opzione non è molto sicura ed è pertanto disabilitata di default.

'Le impostazioni per creare un nuovo utente'
Ogni utente possiede un ID numerico ed uno alfanumerico. La correlazione tra i due viene determinata tramite il file `/etc/passwd` e deve essere univoca. I dati di questa maschera vi aiutano a determinare l'intervallo di cifre da riservare alla parte numerica dell'ID quando si aggiungerà un nuovo utente. Vi consigliamo un intervallo di almeno 500. Cifre generate automaticamente iniziano da 1000. Lo stesso vale per le ID dei gruppi.

'Diverse impostazioni' Per 'Impostazioni dei permessi file' avete tre opzioni: 'Facile', 'Sicuro' e 'Paranoico'. La prima dovrebbe bastare per la maggior parte degli utenti. Consultate anche il testo di aiuto di YaST.

'Paranoico' è un'opzione molto restrittiva, che dovrebbe essere applicata più che altro ad impostazioni proprie dell' amministratore. Se selezionate 'Paranoico', potranno sorgere dei problemi con varie applicazioni, perché gli utenti non avranno più il permesso di accedere a tutta una serie di file. In questo dialogo, potete anche determinare l'utente con il permesso di lanciare il programma `updatedb`. Questo programma viene eseguito automaticamente ogni giorno o dopo il boot e crea una banca dati (locatedb) che contiene la locazione di ogni file del vostro sistema. Se scegliete 'Nessuno', ogni utente avrà accesso solo ai path della banca dati, ai quali hanno

accesso anche tutti gli altri utenti (privi di privilegi). Se selezionate `root` verranno indicizzati tutti i file locali, dal momento che il superutente, ha accesso a tutte le directory. Infine, disattivate l'opzione (default) 'Directory attuale nel path di root' .

Con 'Fine' terminate la configurazione inerente agli aspetti di sicurezza.

Figura 2.9: *Le impostazioni di sicurezza*

2.6.4 Firewall

Questo modulo serve a configurare il SuSEfirewall2 che protegge il vostro sistema da attacchi provenienti da Internet. Informazioni dettagliate sul modo di funzionare di SuSEfirewall2 sono reperibili nella sezione 34.1 a pagina 604.

Suggerimento

Avvio automatico del firewall

YaST avvia automaticamente un firewall su ogni interfaccia di rete configurata con le impostazioni adatte. Dunque, questo modulo dovrete avviarlo solo se volete eseguire delle proprie impostazioni che si spingono oltre alla configurazione di base del firewall, oppure se lo volete disabilitare del tutto.

Suggerimento

2.7 Sistema

2.7.1 Copia di sicurezza di aree del sistema

Il modulo di backup di YaST vi permette di eseguire un backup del vostro sistema. Il modulo non esegue un backup del sistema nel suo intero, bensì solo delle informazioni sui pacchetti modificati, delle aree di sistema cruciali e dei file di configurazione.

Specificate il tipo di dati da includere nel backup. Di solito, vengono salvate tutte le informazioni che riguardano i pacchetti modificati dall'ultima installazione. Potete anche salvare dei file che non appartengono ad alcun pacchetto, come tanti dei file di configurazione sotto `/etc` o le directory della vostra `home`. Inoltre, potrete includere in un backup le aree cruciali del sistema, come la tabella di partizionamento o l'MBR, indispensabili qualora voleste ripristinare il vostro sistema (ingl. restore).

2.7.2 Ripristinare il sistema

Il modulo di ripristino (si veda la figura 2.10 nella pagina successiva) vi permette di ricostruire il vostro sistema da un archivio di backup. Seguite le istruzioni di YaST. Con 'Prossimo', passate da un dialogo all'altro. Iniziate con l'indicazione della locazione degli archivi (supporti rimuovibili, dischi rigidi locali o file system di rete). In seguito verranno visualizzati descrizione e contenuto degli archivi così da poter stabilire cosa ripristinare dagli archivi.

Vi è inoltre una finestra dialogo in cui poter disinstallare dei pacchetti che si sono aggiunti dall'ultimo backup ed una per installarne nuovamente degli altri

eliminati dall'ultimo backup. In questo modo, è possibile ripristinare il sistema esattamente così come era al momento dell'ultimo backup.

Avvertimento

Ripristinare il sistema

Dato che con questo modulo si installano, sostituiscono e cancellano molti pacchetti e file, utilizzatelo solo se disponete già di una certa esperienza in fatto di backup, altrimenti rischiate che si verifichi una perdita di dati.

Avvertimento

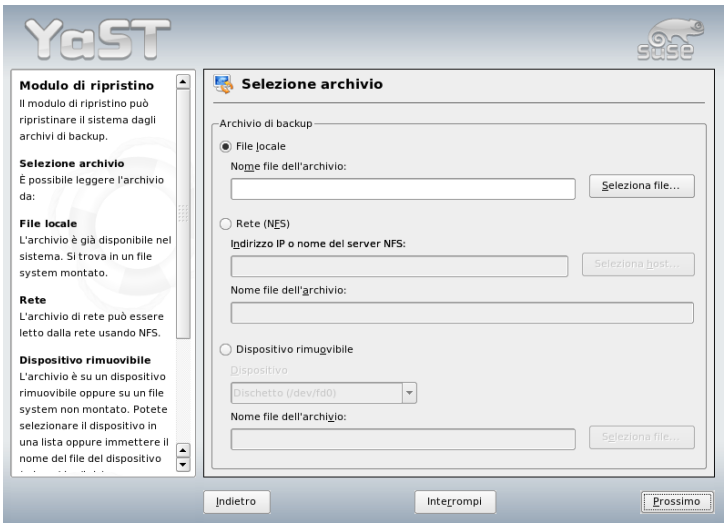

Figura 2.10: *Finestra iniziale del modulo di ripristino*

2.7.3 Creare un dischetto di boot e di salvataggio

Con questo modulo di YaST potete creare facilmente dei dischetti di avvio e di salvataggio. Sono tutti dischetti utili quando si tratta di riparare un sistema se la configurazione del boot risulti danneggiata. Il dischetto di salvataggio

viene usato soprattutto quando è il file system della partizione root ad essere danneggiato.

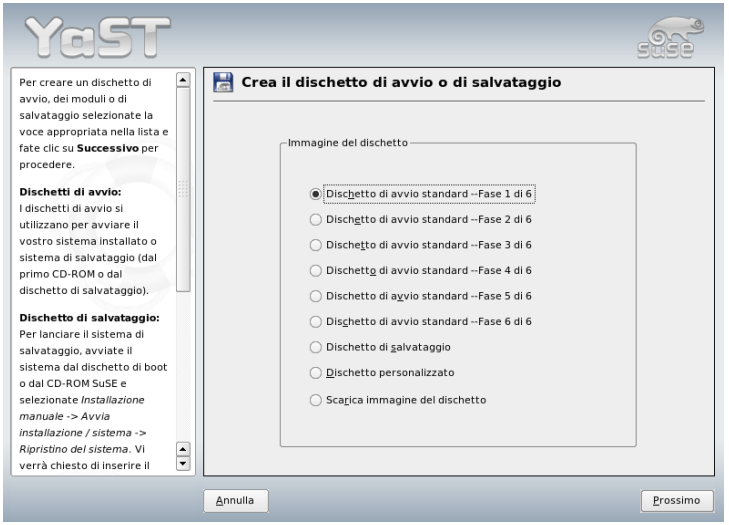

Figura 2.11: *Creare un dischetto di boot e di salvataggio*

Sono disponibili le seguenti opzioni:

'Dischetto di boot standard' Questa opzione crea un dischetto di boot standard che vi permette di inizializzare un sistema già installato. In base all'architettura, il numero dei dischetti di boot può variare, si consiglia di creare tutti i dischetti di boot riportati nella finestra, perché sono tutti necessari per il processo di boot. I dischetti possono essere anche usati per avviare il sistema di salvataggio.

'Dischetto di salvataggio' Questo dischetto contiene un'ambiente speciale che vi permette di eseguire dei lavori di manutenzione nel vostro sistema installato. Esempio di tali interventi sono la verifica e la messa a punto del file system, nonché l'aggiornamento del bootloader. Per inizializzare il sistema di salvataggio, avviate il sistema con il dischetto di boot e selezionate 'Installazione manuale' → 'Avvia installazione/sistema' → 'Sistema di salvataggio' Vi verrà chiesto di inserire il dischetto di salvataggio nel lettore.

'Dischetti personalizzati' Con questa opzione potete scrivere un'image qualsiasi già esistente dal disco rigido su dischetto.

'Scarica image di dischetto' Indicate un URL ed i vostri dati di autenticazione e scaricate un'image di dischetto da Internet.

Per creare uno dei dischetti appena descritti, selezionate la relativa opzione e cliccate su 'Avanti'. Vi verrà chiesto di inserire un dischetto. Cliccate ancora una volta su 'Prossimo' e verrà creato il dischetto.

2.7.4 LVM

Il Logical Volume Manager (LVM) è uno strumento che consente di eseguire un partizionamento personalizzato dei dischi rigidi con drive logici. Per maggiori dettagli in tema di LVM consultate la sezione 3.6 a pagina 98.

2.7.5 Partizionare

Nella finestra per esperti (si veda la figura 2.12 nella pagina successiva), potete partizionare manualmente il vostro disco rigido. Potete aggiungere, eliminare o modificare delle partizioni. Da questo modulo YaST potete anche accedere alle finestre di configurazione di soft RAID e LVM.

Avvertimento

Anche se è possibile modificare le partizioni del sistema installato, questo intervento va eseguito solo da utenti esperti, altrimenti vi è il rischio che in caso di errore si verifichi una perdita di dati. Se modificate il partizionamento di un disco mentre viene utilizzato, riavviate in seguito il sistema. E' più sicuro utilizzare il sistema di salvataggio che eseguire il ripartizionamento del sistema in esecuzione.

Avvertimento

Nell'elenco della finestra per esperti troverete tutte le partizioni di tutti i dischi rigidi del vostro computer. I dischi interi vengono rappresentati come dispositivi senza numero (es.: `/dev/hda` o `/dev/sda`), mentre le singole partizioni vengono numerate in quanto parte di questi dischi (ad es. `/dev/hda1` o `/dev/sda1`). La lista riporta i parametri più importanti delle partizioni e dei dischi, ovvero dimensioni, tipo, file system e punto di mount. Il punto di mount indica il punto in cui la partizione è montata nell'albero dei file di Linux.

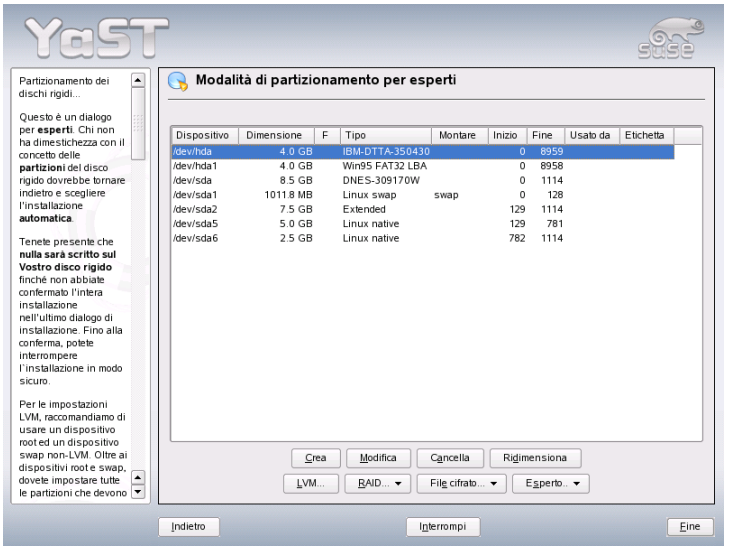

Figura 2.12: *Il partizionatore di YaST per esperti*

Se in fase di installazione lanciate il dialogo per esperti viene mostrato anche lo spazio disponibile (se ve n'é) e automaticamente selezionato. Se desiderate dare più spazio a SUSE LINUX potete assegnarli una partizione di un disco rigido, partendo dall'ultima fino ad arrivare alla prima. Comunque se si hanno tre partizioni, tuttavia, non sarà possibile assegnare solo la seconda a SUSE LINUX e riservare la prima e la terza ad altri sistemi operativi.

Creare una partizione

Selezionate 'Crea'. Se si hanno più di un disco rigido, appare un dialogo con una lista dei dischi rigidi. Sceglietene uno per la vostra nuova partizione. Dopodiché, impostate il tipo di partizione (primaria o estesa). Potete creare fino a quattro partizioni primarie o tre primarie ed un'estesa. La partizione estesa può, a sua volta, essere suddivisa in partizioni logiche (si veda la sezione Tipi di partizioni a pagina 11).

Scegliete poi un file system con cui formattare la partizione e, se necessario, anche un punto di mount. YaST ve ne propone uno per ogni nuova partizione. Cliccate su 'OK' per applicare le modifiche. La nuova partizione verrà ora inserita nella

tabella delle partizioni. Se cliccate su 'Prossimo', i parametri vengono applicati e riappare la schermata delle proposte.

I parametri del partizionamento

Quando create una nuova partizione o ne modificate una preesistente, potete impostare una serie di valori nel partizionatore. Per le partizioni nuove, vi consigliamo di accettare i parametri proposti da YaST. Altrimenti, procedete come segue:

1. Selezionare la partizione.
2. Modificare la partizione ed impostare i parametri.

   ID del file system Se non avete ancora intenzione di formattare la partizione, precisate qui almeno l'ID del file system, in modo da poter eseguire correttamente il mount della partizione; valori possibili sono ad es. 'Linux', 'Linux swap', 'Linux LVM' e 'Linux RAID'. Per maggiori informazioni su LVM e RAID rimandiamo alla sezione 3.6 a pagina 98 e alla sezione 3.7 a pagina 105.

   File system Se, invece, avete intenzione di formattare la partizione durante l'installazione, precisate il file system della partizione, avete la scelta tra 'Swap', 'Ext2', 'Ext3', 'ReiserFS' e 'JFS'. I singoli file system sono illustrati nel capitolo 20 a pagina 373.

   Swap è un formato speciale che permette di utilizzare una partizione come memoria virtuale. ReiserFS è il default in Linux. ReiserFS, JFS e Ext3, sono dei cosiddetti "Journaling File system". Questo tipo di file system riesce a ripristinare rapidamente il sistema dopo un crollo, perché i processi di scrittura vengono protocollati mentre il sistema è in esecuzione. Inoltre, ReiserFS è velocissimo a gestire grandi quantità di piccoli file. Ext2 non è un Journaling File system, ma è molto stabile ed ottimo per piccole partizioni, dal momento che non richiede molto spazio.

   Opzioni per file system Questo dialogo contiene diversi parametri per il file system selezionato. Queste impostazioni, a seconda del tipo di file system, possono essere molto complesse e si consiglia solo ad esperti di metterci mano.

   Cifrare il file system Se attivate la cifratura, tutti i dati verranno salvati in modo cifrato sul disco rigido. Questo procedimento aumenta la sicurezza dei dati più importanti, ma richiede del tempo. Per maggiori dettagli a riguardo proseguite con la sezione 34.3 a pagina 619.

Le opzioni Fstab In questo dialogo, potete indicare i parametri dei file di amministrazione dei file system (`/etc/fstab`).

Il punto di mount Indica la directory dove poter montare la partizione nell'albero dei file. YaST vi fa alcune proposte che se applicate strutturano il vostro file system secondo lo standard, oppure potete anche utilizzare nomi di vostra invenzione.

3. Con 'Prossimo' attivate la partizione.

Se decidete di partizionare manualmente, impostate sempre una partizione swap di almeno 256 Mbyte. L'area swap serve a immagazzinare tutti quei dati momentaneamente non necessari, alleggerendo la RAM e tenendola libera per i dati più utilizzati.

Opzioni per esperti

'Per esperti...' apre un menu contenente i seguenti comandi:

Rileggi tabella delle partizioni Processo necessario dopo aver eseguito il partizionamento manuale nella console di testo.

Elimina tabella delle partizioni ed etichetta del disco
In tal modo sovrascrivete la vecchia tabella delle partizioni. Ad esempio, ciò può essere utile se incontrate delle difficoltà con etichette non convenzionali. Con questo approccio vengono cancellati tutti i dati sul disco rigido.

Ulteriori indicazioni sul partizionamento

Quando si partiziona il disco automaticamente e vengono rilevate altre partizioni nel sistema, queste saranno incluse nel file `/etc/fstab` per permettere, in un secondo momento, di accedere più facilmente a questi dati. Questo file contiene altre partizioni del sistema con tutti i loro parametri (come tipo di file system, punto di mount e permessi degli utenti).

Esempio 2.1: */etc/fstab: le partizioni data*

```
/dev/sda1       /data1  auto    noauto,user 0 0
/dev/sda5       /data2  auto    noauto,user 0 0
/dev/dasda6     /data3  auto    noauto,user 0 0
```

Tutte le partizioni, sia Linux che FAT, vengono montate con le opzioni `noauto` e `user`. In questo modo, tutti gli utenti possono smontarle in caso di necessità. Per motivi di sicurezza, YaST non usa l'opzione `exec`, che serve, però, ad eseguire programmi dalla partizione. Se avete intenzione di eseguire programmi o script, aggiungete voi questa opzione. Questa misura si renderà utile, se non altro, quando vi arriveranno dei messaggi come bad interpreter o Permission denied.

Partizionare e LVM

Dal partizionatore per esperti giungete alla configurazione di LVM tramite 'LVM' (si veda la sezione 3.6 a pagina 98). Comunque, se sul vostro sistema vi è già una configurazione LVM funzionante, essa verrà attivata automaticamente non appena entrate per la prima volta in una sessione nelle finestre di configurazione di LVM. In questo caso, un disco che contiene una partizione appartenente ad un gruppo di volume abilitato non potrà essere ripartizionato, poiché il kernel di Linux non rilegge una tabella delle partizioni modificata di un disco rigido se una delle partizioni del disco viene utilizzata. Comunque se sul vostro sistema vi è già una configurazione LVM funzionante, non dovrebbe essere necessario eseguire un ripartizionamento. Modificate invece la configurazione dei volumi logici.

All'inizio di un volume fisico (ingl. physical volume, abbr. con PV), trovate delle indicazioni sul volume scritte nella partizione, in modo che un PV "sappia" a quale gruppo appartiene. Per riutilizzare una partizione del genere per scopi che non hanno nulla a che vedere con LVM, è consigliabile cancellare l'inizio del volume. Ad esempio nel gruppo volumi `system` e PV `/dev/sda2`, ciò si realizza con `dd if=/dev/zero of=/dev/sda2 bs=512 count=1`.

Avvertimento

File System per il boot

Il file system utilizzato per il boot (il file system root o `/boot`) non può trovarsi su un volume logico LVM. Specificate a tal fine invece una normale partizione fisica.

Avvertimento

2.7.6 Il profile manager (SCPM)

Il modulo dell'SCPM (ingl. System Configuration Profile Management) vi permette di impostare, amministrare e di passare all'occorrenza da una configura-

zione del sistema all'altra. Questa opzione è particolarmente utile su computer portatili usati in ambienti diversi (in reti diverse) e da persone diverse. Tuttavia, grazie a questo modulo, anche su sistemi desktop si potrà sperimentare con diversi componenti hardware e configurazioni prova. Per degli approfondimenti in tema di SCPM rimandiamo al capitolo 15 a pagina 295.

2.7.7 Editor dei runlevel

SUSE LINUX presenta diversi runlevel, detti anche livelli di esecuzione. Il runlevel 5 è quello standard; si tratta del livello multiutente con superficie grafica (il sistema X-Window) e accesso alla rete. Vi sono anche il runlevel 3 (modo multiutente con rete, senza X), il runlevel 2 (modo multiutente senza rete), i runlevel 1 e S (ad utente singolo), lo 0 (il runlevel di spegnimento del sistema) ed il 6 (reboot del sistema).

I diversi runlevel sono stati ideati per risolvere eventuali problemi riscontrati con determinati servizi (X o rete) nei runlevel più alti. Infatti, in un caso del genere, essi permettono di caricare il sistema in un runlevel inferiore e da lì si potrà riparare il servizio causa di difficoltà. Inoltre, molti server non dispongono di una superficie grafica, il che vuol dire che vanno caricati, ad esempio, nel runlevel 3.

Solitamente vi servirà solo il runlevel (5). Però, se la superficie grafica dovesse bloccarsi, potete riavviare l'X window system passando alla console di testo. con Ctrl-Alt-F1, immettervi come root e passare al runlevel tre (con il comando `init 3`). Con il runlevel 3 viene spento il sistema X-Window e avete solo una console di testo. Per riavviare la superficie grafica, basta un `init 5` per tornare nel runlevel 5.

Per maggiori informazioni sui runlevel in SUSE LINUX ed una descrizione del editor dei runlevel di YaST rimandiamo al capitolo 7 a pagina 159.

2.7.8 Editor sysconfig

La directory `/etc/sysconfig` contiene i file con le impostazioni più importanti per SUSE LINUX. L' editor sysconfig vi elenca tutte le opzioni di configurazione. I parametri possono essere modificati e poi salvati nei singoli file di configurazione. In linea di massima non è necessario apportare delle modifiche manualmente, dal momento che i file vengono aggiornati automaticamente ogni volta che si installa un pacchetto o si configura un servizio. Per ulteriori informazioni su `/etc/sysconfig` e sull' editor sysconfig di YaST rimandiamo al capitolo 7 a pagina 159.

2.7.9 Selezionare il fuso orario

Il fuso orario viene impostato durante l'installazione. In questo dialogo, potete modificarlo. Selezionate la vostra nazione dalla lista e cliccate su 'Ora locale' o 'UTC'(Universal Time Coordinated, in passato Greenwich Mean Time). Sotto Linux si usa di solito 'UTC'. Altri sistemi operativi come Microsoft Windows usano per lo più l'ora locale.

2.7.10 Selezionare la lingua

Qui potete intervenire sull'impostazione della lingua; le impostazioni di YaST valgono per tutto il sistema, quindi anche per YaST ed l' ambiente desktop.

2.8 Vari

2.8.1 Contattare il servizio di supporto

Acquistando SUSE LINUX potrete usufruire gratuitamente del servizio di supporto all'installazione. Per saperne di più (temi contemplati, indirizzo e numero di telefono), andate sul nostro sito `http://www.novell.com/linux/suse/`.

YaST vi permette di contattare il team SUSE direttamente per e-mail, dopo aver registrato il vostro sistema. Inserite innanzitutto i vostri dati (troverete il codice di registrazione sul retro della custodia del CD). Per quanto riguarda la domanda che desiderate porre al servizio di supporto, passate alla finestra successiva e scegliete la categoria a cui appartiene il vostro problema. Descrivete quindi il problema (si veda la figura 2.13 nella pagina successiva). Fatevi consigliare anche da YaST: le sue istruzioni vi aiutano a formulare le vostre domande in modo tale che il team di supporto possa aiutarvi nel modo più veloce possibile.

Suggerimento

Per richieste di supporto che vanno oltre alle tematiche inerenti all'installazione, visitate il sito `http://support.novell.com/linux/` per avere maggiori informazioni.

Suggerimento

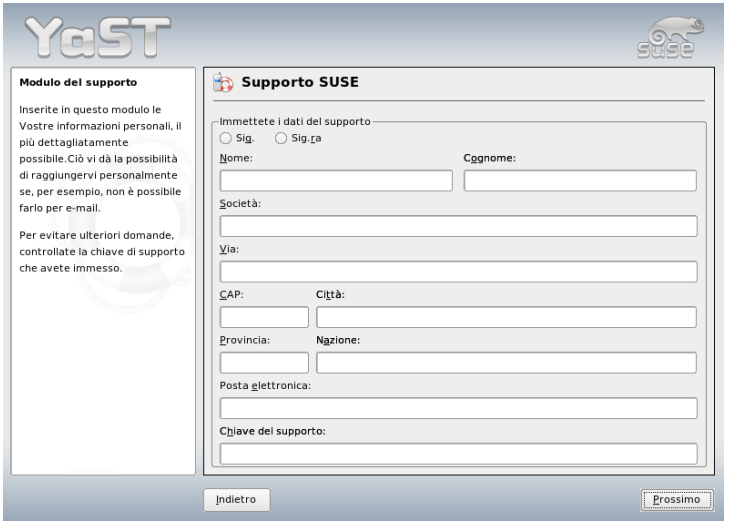

Figura 2.13: *Contattare il servizio di supporto*

2.8.2 Protocollo di avvio

Il file di protocollo del processo di boot `/var/log/boot.msg` contiene i messaggi che scorrono sullo schermo durante la fase di avviamento del sistema. Questo modulo di YaST vi permette di visualizzarli e di verificare, ad esempio, se tutti i servizi e le funzionalità siano stati caricati correttamente.

2.8.3 Il protocollo di sistema

Il file di protocollo del sistema `/var/log/messages` documenta il funzionamento del vostro computer. I messaggi del kernel vi sono elencati in ordine cronologico.

2.8.4 Caricare il CD dei driver del produttore

Questo modulo vi permette di installare automaticamente i driver per SUSE LINUX. da un CD di driver per SUSE LINUX. Quando installate SUSE LINUX di

sana pianta usate questo modulo di YaST per caricare driver necessari dal CD del produttore.

2.9 YaST nel modo testo (ncurses)

Questa sezione si rivolge soprattutto ad amministratori di sistema e utenti avanzati che lavorano con computer su cui non gira un X server e che quindi possono eseguire una installazione solo nel modo testo. In questa sezione verrà illustrato l'uso di YaST nel modo testo (ncurses).

Se avviate YaST nel modo testo verrà visualizzato come prima cosa il centro di controllo di YaST (si veda la figura 2.14 in questa pagina). Avrete tre settori: sulla sinistra incorniciata di bianco avete le categorie dei singoli moduli. La categoria abilitata si distingue per il colore. Sulla destra vedete una rassegna, lievemente incorniciata di bianco, dei moduli contenuti nella categoria abilitata. In basso avete i bottoni 'Aiuto' e 'Esci'.

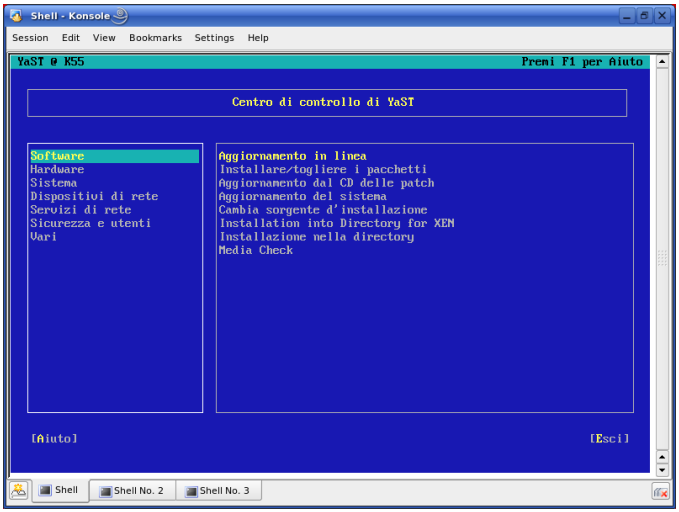

Figura 2.14: *La finestra principale di YaST nel modo testo*

Dopo il primo l'avvio del centro di controllo di YaST il cursore si trova su 'Software'. Con ↓ e ↑ passate da una categoria all'altra. Per avviare un modulo della

categoria selezionata, usate il tasto (→). Nel riquadro a destra vedete ora i moduli di questa categoria. Selezionate il modulo tramite i tasti (↓) e (↑). Appena selezionato, il modulo assume un colore diverso, e in basso vedrete una breve descrizione del modulo.

Con (Invio) potete lanciare il modulo selezionato. Ci sono dei bottoni o campi di selezione che presentano una lettere di un colore diverso, giallo di default. Con la combinazione di (Alt)–(lettera gialla) potete selezionare il bottone direttamente senza dover ricorrere a (Tab). Per uscire dal centro di controllo di YaST vi è il bottone 'Esci', oppure selezionate la sotto-voce'Esci' nella panoramica delle categorie e premete (Invio).

2.9.1 Navigare all'interno dei moduli

Nella seguente descrizione dei singoli elementi dei moduli si parte dal presupposto che i tasti funzione e le combinazioni di tasti con (Alt) funzionano e non sono già mappati. Per le possibili eccezioni vi rimandiamo alla sezione 2.9.2 nella pagina successiva.

Navigare tra i bottoni/liste di selezione:
Con (Tab) e (Alt)–(Tab) o (Shift)–(Tab) potete navigare tra i diversi bottoni e/o riquadri delle liste di selezione.

Navigare nella lista di selezione: Con i tasti freccia ((↑) e (↓)) selezionate i singoli elementi nel riquadro attivo in cui si trova una lista di selezione. Se delle singole voce all'interno di un riquadro dovessero non rientrare per la loro larghezza nel riquadro, utilizzate (Shift)–(→) o (Shift)–(←) per spostarsi orizzontalmente verso destro e sinistra (alternativamente funziona anche (Ctrl)–(e) o (Ctrl)–(a)). Questa combinazione funziona anche in quei casi dove un semplice (→) o (←) comporterebbe un cambio del riquadro attivo o della lista della selezione come nel centro di controllo.

Bottoni, radio bottoni e check box Per selezionare bottoni con una parentesi quadra vuota (check box) o con le parentesi tonde (radio bottoni) servitevi della (Barra Spaziatrice) o date (Invio). Alternativamente potete selezionare in modo mirato radio bottoni e checkbox tramite (Alt)–(Lettera_gialla). In questo caso non serve confermare ancora una volta con (Invio). Tramite il tasto (Tab) è necessario un ulteriore (Invio), affinché l'azione selezionata venga eseguita o la relativa voce di menu abilitata.

I tasti funzione I tasti funzione (F1 - F12) vi permettono di indirizzare direttamente dei bottoni. La funzione eseguita dal tasto dipende dal modulo YaST nel quale vi trovate, visto che nei diversi moduli sono disponibili diversi bottoni (p.es. dettagli, informazioni, aggiungi, cancella ...). Con F10 date 'OK', 'Prossimo' e 'Fine'. In YaST con il tasto F1 vi potete fare indicare le funzioni dei tasti funzione.

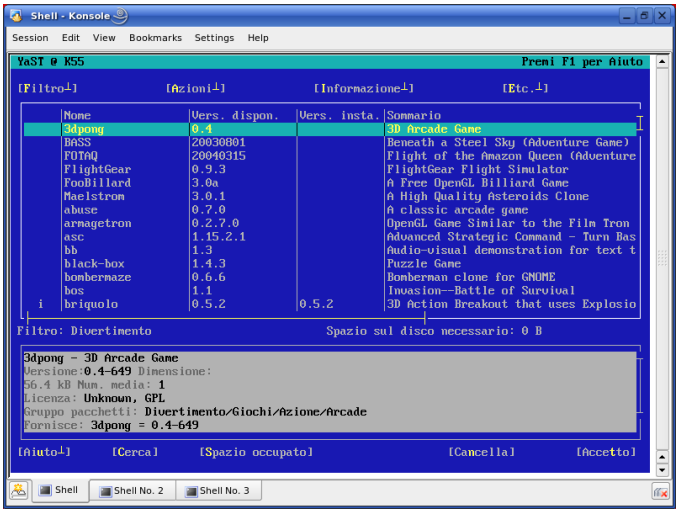

Figura 2.15: *Il modulo per l'installazione del software*

2.9.2 Restrizioni riguardanti la combinazione dei tasti

Se sul vostro sistema con l' X server in esecuzione esistono delle combinazioni di tasti con Alt, può verificarsi che le combinazioni con Alt non funzionino in YaST. Inoltre, tasti come Alt o Shift possono essere già occupati da impostazioni del terminale.

Sostituire Alt con Esc: Le combinazioni di tasti con Alt possono essere eseguite con Esc; al posto di Alt–h si ha la combinazione dei tasti Esc–h.

Spostarsi in avanti o indietro con Ctrl–f e Ctrl–b:
Se le combinazioni con Alt e Shift sono già mappate dal window manager o dal terminale, avete la possibilità di usare in alternativa le combinazioni Ctrl–f (avanti) e Ctrl–b (indietro).

Restrizioni dei tasti funzione: Se alcuni tasti di funzione sono già occupati dal terminale e non sono quindi disponibili per YaST, in una console puramente testuale le combinazioni con Alt ed i tasti funzione dovrebbero essere comunque tutti disponibili.

2.9.3 Richiamare singoli moduli

Per risparmiare del tempo, ogni modulo di YaST può essere richiamato singolarmente, basta immettere: `yast nomemodulo`. Il modulo di rete p.es. si avvia con `yast lan`. Una lista dei nomi dei moduli che sono disponibili nel vostro sistema, si ottiene con il comando `yast -l` o tramite `yast --list`.

2.9.4 Il modulo YOU

Potete lanciare YOU anche dalla riga di comando come ogni altro modulo YaST immettendo da `root`

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

Con `yast2 online_update` invocate il rispettivo modulo. Con l'indicazione facoltativa di una `url` indicate a YOU un server (locale o su Internet) da cui scaricare le patch ed informazioni. Se non indicate una URL all'avvio del modulo, selezionate il server/ la directory tramite la maschera di YaST. Come per la versione grafica di YaST anche qui potete impostare un job di cron tramite il bottone 'Configura l'aggiornamento in modo automatico'.

2.10 Aggiornamento in linea dalla linea di comando

Potete ricorrere a online_update, un tool a linea di comando, per eseguire un aggiornamento del tutto automatico del sistema (p. es tramite degli script). Partiamo dal presupposto che vogliate che il vostro sistema rilevi un determinato

server su cui si trovano degli aggiornamenti e scaricare quindi delle patch con le relative note ad un ora prestabilita e ad intervalli regolari. Comunque non volete che le patch vengano installate automaticamente, prima di proseguire con l'installazione le volete prendere in visione.

Per poter ricorrere a questo strumento dovete prima impostare un job di cron che esegue il seguente comando:

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

`-u` introduce l'URL di base dell'albero delle directory dal quale scaricare le patch. I protocolli supportati sono: `http`, `ftp`, `smb`, `nfs`, `cd`, `dvd`, e `dir`. `-g` scarica le patch archiviandole senza però installarle in una directory locale. Potete anche applicare un filtro alle patch specificandone la categoria: `security`, `recommended` o `optional`. Se in tal senso non specificate alcunché, online_update scaricherà tutte le nuove patch delle categorie `sicurezza` e `raccomandate`.

I pacchetti scaricati possono essere installati immediatamente senza prendere visione delle singole patch. online_update salva le patch nella directory `/var/lib/YaST2/you/mnt`. Per installare le patch, eseguite il seguente comando:

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

Il parametro `-u` specifica l'URL (locale) della patch da installare. `-i` avvia il procedimento di installazione.

Per visionare le patch scaricate prima di proseguire con l'installazione lanciate la finestra di YOU:

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

Al suo avvio YOU andrà a cercare le patch scaricate in precedenza nella directory locale invece che su Internet. Non vi resta che selezionare le patch da installare.

Durante l'aggiornamento in linea di YaST è possibile specificare dei parametri dalla linea di comando. La sintassi da seguire in questi casi è `online_update [parametro dalla linea di comando]`. I parametri a vostra disposizione e le loro funzionalità vengono illustrati di seguito.

`-u URL` URL di base dell'albero delle directory da cui scaricare le patch.

`-g` Scaricare solamente le patch senza installarle.

-i Installa patch scaricate. Non eseguire download.

-k Verifica la presenza di nuove patch.

-c Mostra solo configurazione attuale, senza eseguire alcunché.

-p prodotto Il prodotto per il quale scaricare le patch.

-v versione Versione del prodotto per la quale scaricare le patch.

-a architettura Architettura di base di un prodotto per la quale scaricare delle patch.

-d Scarica le patch e simula l'installazione (il sistema rimane invariato, solamente a fine di prova).

-n Nessuna verifica della firma dei file scaricati.

-s Mostra elenco delle patch disponibili.

-V Verbosità.

-D Modo per esperti e la risoluzione di problemi.

Per maggiori informazioni riguardanti online_update, immettete `online_update -h`.

Particolari varianti di installazione

SUSE LINUX si lascia installare in vario modo, velocemente nel modo grafico o anche nel modo di testo, variante che vi permette di eseguire una serie di adattamenti manuali. Segue una presentazione delle varianti di installazione particolari nonché del modo di utilizzare diverse fonti di installazione (CD-Rom, NFS). In questo capitolo troverete anche dei consigli su come risolvere eventuali problemi di installazione. Il capitolo si chiude con una sezione dettagliata dedicata al partizionamento.

3.1 linuxrc

Ogni sistema presenta delle routine BIOS particolari che vengono eseguite all'avvio del sistema e per inizializzare l'hardware. Durante il processo di boot, queste routine, caricano un' immagine che viene eseguita dal sistema. Questa immagine è di solito un boot manager che permette di selezionare un sistema installato o un sistema di installazione. Durante l'installazione di SUSE LINUX viene caricata una boot image che contiene il kernel ed un programma chiamato "linuxrc".

linuxrc è un programma che analizza e inizializza il sistema ai fini dell'installazione. Di default, il tutto si svolge senza l'intervento da parte dell'utente. linuxrc, dopo aver eseguito un'analisi del sistema, avvia YaST Se dovete passare dei parametri ai moduli, o se il rilevamento dell'hardware dovesse fallire potrebbe rendersi necessario eseguire linuxrc in modo interattivo avviando l'installazione manuale.

linuxrc può essere utilizzato non solo per l'installazione, ma anche come strumento di caricamento di un'altro sistema installato. Potete persino avviare un sistema autonomo di salvataggio basato sulla ramdisk, per informazioni dettagliate consultate la sezione 5.4 a pagina 147.

Se il sistema utilizza un initial RAM disk (initrd), uno shell script chiamato linuxrc gestisce il caricamento dei moduli al momento del boot. Questo script viene generato in modo dinamico dallo script `/sbin/mkinitrd`, che non va assolutamente confuso con il programma linuxrc utilizzato in fase di installazione.

3.1.1 Passare dei parametri a linuxrc

Sussiste la possibilità di passare dei parametri a linuxrc che permettono di intervenire sul processo di avviamento. linuxrc cerca di rilevare un file info sul dischetto o nel file `initrd` sotto `/info`. Solo in seguito linuxrc legge i parametri al prompt del kernel. I valori preimpostati possono essere modificati nel file `/linuxrc.config` che verrà caricato come primo. Comunque si consiglia di eseguire le modifiche nel file info.

Suggerimento

Potete eseguire linuxrc nel modo manuale immettendo al prompt di installazione il parametro "manual=1".

Suggerimento

Un file info è composto da parole chiave e rispettivo valore: `key: value`. Queste coppie composte da chiave/valore possono essere immesse anche al prompt di boot dell'origine di installazione seguendo questa sintassi `key=value`. Il file `/usr/share/doc/packages/linuxrc/linuxrc.html` contiene l'elenco di tutte le chiavi. Ecco alcune di rilievo:

Install: URL (nfs, ftp, hd, ...) Specifica la fonte di installazione come URL. Protocolli consentiti: `cd`, `hd`, `nfs`, `smb`, `ftp`, `http` e `tftp`. La sintassi è quella comune, ad es.:

- `nfs://<server>/<directory>`
- `ftp://[utente[:password]@]<server>/<directory>`

Netdevice: <eth0> Se disponete di diversi dispositivi Ethernet tramite il parametro `Netdevice:` potete selezionare l'interfaccia che debba utilizzare linuxrc.

HostIP: <10.10.0.2> In tal modo stabilite l'indirizzo IP dell'host.

Gateway: <10.10.0.128> Se il server di installazione non si trova nella stessa sottorete dell'host, specificate tramite quale gateway possa essere indirizzato.

Proxy: <10.10.0.1> Per il tipo di connessione ftp e http potete utilizzare anche un Proxy. A tal fine dovete indicarlo tramite il parametro `Proxy:`.

ProxyPort: <3128> Se il proxy non utilizza la porta di default, potete stabilire con questa opzione la porta necessaria.

Textmode: <0|1> Utilizzate questo parametro per avviare YaST nel modo di testo.

VNC: <0|1> Per eseguire il processo di installazione comodamente anche su host sprovvisti di console grafica potete eseguire l'installazione tramite VNC. Il parametro `VNC` consente di controllare il processo di installazione tramite VNC. Se abilitato, il rispettivo servizio viene attivato sul sistema di installazione. Confrontate anche il parametro `VNCPassword`.

VNCPassword: <password> Imposta la password per l'installazione eseguita tramite VNC in modo da controllare l'accesso alla sessione.

UseSSH: <0|1> Consente di accedere a linuxrc tramite SSH per un'installazione tramite YaST nel modo testo.

SSHPassword: <password> Imposta la password per l'utente `root` per poter accedere a linuxrc.

Insmod: <modulo> <parametro> Indicazione del modulo da caricare da parte del kernel e dei parametri richiesti. I parametri del modulo vanno divisi da spazi.

AddSwap: <0|3|/dev/hda5> Con 0 non verrà richiesta alcuna partizione swap, nel caso di un numero positivo viene attivata la partizione corrispondente al numero. Alternativamente potete indicare il nome della partizione.

3.2 Installare tramite VNC

VNC (*Virtual Network Computing*) è una soluzione client-server che consente di gestire in modo intuitivo un X-server remoto tramite un client snello e semplice da maneggiare. Il client è disponibile per diverse piattaforme come ad esempio per diverse versioni di Microsoft Windows, MacOS di Apple e Linux.

ll VNC-client, vncviewer viene utilizzato per realizzare la visualizzazione grafica ed il controllo di YaST durante il processo di installazione. Prima dell'avvio del sistema da installare il sistema remoto dovrà disporre dell'accesso tramite rete al sistema da installare.

3.2.1 Preparativi per l'installazione tramite VNC

Per eseguire una installazione tramite VNC vanno passati alcuni parametri al kernel, cosa che va fatta prima dell'avvio del kernel. Passate a riguardo le seguenti opzioni al prompt di boot:

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

`vnc=1` segnala che il server VNC sta per essere lanciato sul sistema di installazione. Tramite `vncpassword` definite la password da utilizzare nel proseguio

del processo di installazione. La fonte di installazione (`install`) può venir indicata manualmente (indicazione del protocollo e dell'URL della directory in questione) oppure contenere l'istruzione `slp:/`. In questo caso la fonte di installazione viene determinata automaticamente tramite una richiesta SLP; per avere ulteriori dettagli su SLP consultate al capitolo 23 a pagina 441.

3.2.2 I client e l'installazione tramite VNC

La connessione al sistema da installare e al server VNC in esecuzione su tale sistema viene creata tramite un client VNC. SUSE LINUX ricorre a vncviewer che trovate nel pacchetto `xorg-x11-Xvnc`. Se desiderate creare la connessione verso il sistema da installare partendo da un client Windows dovete installare sul sistema Windows il programma tightvnc che trovate sul primo CD di SUSE LINUX nella directory `/dosutils/tightvnc`.

Avviate un client VNC di vostra scelta ed indicate l'indirizzo IP del sistema da installare nonché la password VNC quando il programma ve lo richiede.

Come alternativa potete creare la connessione VNC anche tramite un browser Java compatibile. In questo caso dovete immettere nel campo di indirizzo del browser:

```
http://<indirizzo_IP_del_sistema_da_installare>:5801/
```

Una volta creata la connessione, si avvia ed il processo di installazione può avere inizio.

3.3 L'installazione in modalità testo con YaST

Oltre all'installazione tramite l'interfaccia grafica, SUSE LINUX può essere installato nel modalità testo con YaST (modo di console). Tutti i moduli di YaST sono disponibili anche nella modalità testo. La modalità testo è particolarmente utile quando non si ha bisogno di un'interfaccia grafica (sistemi server), oppure quando il sistema X Window non supporta la scheda grafica. E infine, questa modalità di installazione assieme ai relativi dispositivi di emissione consente agli utenti ipovedenti di eseguire l'installazione di SUSE LINUX.

Innanzitutto, si deve impostare la sequenza di boot nel BIOS in modo che il sistema si avvii dal lettore CD-ROM o DVD. Inserite quindi il DVD o il CD 1 nel lettore e riavviate il PC. Dopo un paio di secondi apparirà la schermata di avvio.

Selezionate, servendovi dei tasti ↑ e ↓ (entro 10 secondi) 'Installazione manuale', in modo che *non* venga avviato automaticamente il sistema installato. Nella riga `boot options` eventualmente inserite i parametri del kernel, se il vostro hardware li richiede. Normalmente comunque non sussiste la necessità. Se selezionate quale lingua di installazione quella della vostra tastiera verrà impostata correttamente anche la mappatura della tastiera, semplificando quindi l'inserimento dei parametri.

Coi tasti F2 ('Video mode') impostate la risoluzione dello schermo per l'installazione. Selezionate 'Text Mode' per passare al modo di testo se la scheda grafica crea delle difficoltà durante l'installazione. Infine premete Invio. Appare ora una finestra di dialogo che vi mostra lo stato di progressione (Loading Linux kernel); poi, si avvia il kernel e linuxrc. Il programma linuxrc si basa su menu e attende l'immissione di comandi da parte dell'utente.

Una serie di difficoltà durante la fase di caricamento possono essere solitamente risolte con alcuni parametri del kernel. In caso di problemi dovuti al DMA, usate l'opzione di avvio 'Installation - Safe Settings'.

In caso di difficoltà dovute ad ACPI (ingl. Advanced Configuration and Power Interface) disponete dei seguenti parametri del kernel:

`acpi=off` Questo parametro disattiva completamente il sistema ACPI, indicato se il vostro computer non supporta ACPI o pensate che l'implementazione ACPI crei dei problemi.

`acpi=oldboot` Disattiva quasi completamente il sistema ACPI, rimangono attive solo quelle parti necessarie al processo di boot.

`acpi=force` Attiva l'ACPI anche se il BIOS del vostro computer risale agli anni antecedenti al 2000. Questo parametro sovrascrive `acpi=off`.

`pci=noacpi` Questo parametro disabilita il PCI IRQ-routing del nuovo sistema ACPI.

Vedete anche il relativo articolo della banca dati di supporto redatto in inglese che trovate eseguendo una ricerca su `https://portal.suse.com` servendovi della parola chiave *acpi*.

Selezionate 'Memory Test', per una verifica della memoria, in caso si dovessero verificare delle difficoltà "inspiegabili" in fase di caricamento del kernel o durante l'installazione. Linux è molto esigente in quanto ad hardware: la memoria ed il suo timing devono essere ineccepibili! Per maggiori approfondimenti, rimandiamo agli articoli che trattano questa tematica che troverete eseguendo una ricerca con "memtest86" nella nostra banca dati di supporto. Infine, consigliamo di eseguire il test della memoria durante la notte.

3.4 Consigli e trucchetti

Alcuni computer, non dispongono di un lettore CD-Rom, ma di un lettore di dischetti atto al boot. Per eseguire un'installazione su un sistema del genere, dovete creare un dischetto di boot e utilizzarlo per avviare il vostro sistema.

Vi serve un dischetto 3.5 HD, ovvero ad alta densità, formattato e un lettore floppy 3.5 capace di eseguire il boot. Sul CD 1 nella directory `boot` trovate alcune cosiddette immagini di dischetto (images). Una tale immagine si lascia copiare con delle utility sul dischetto; alla fine di questo procedimento si avrà un dischetto di avvio.

Queste immagini di dischetto contengono inoltre il loader (detto anche caricatore) SYSLINUX e il programma linuxrc. SYSLINUX vi consente di selezionare durante il processo di avvio il kernel desiderato, e di passare all'occorrenza dei parametri dell'hardware impiegato. Il programma linuxrc vi assiste durante il processo di caricamento dei moduli del kernel richiesti per il vostro hardware ed infine lancia il processo di installazione.

3.4.1 Creare un dischetto di boot con rawwritewin

Windows contiene un programma grafico rawwritewin che trovate sul relativo CD 1 nella directory `dosutils\rawwritewin`.

Dopo l'avvio dovete indicare il file immagine che trovate anche sul CD1 nella directory boot. Vi servono almeno le images `bootdisk` e `modules1`. Per visualizzarle nel browser dei file dovete selezionare `allfiles` quale tipo di file. Inserite il dischetto nel lettore e cliccate su 'write'.

In questo modo potete creare anche le altre immagini di dischetti `modules1` e `modules2` `modules3` e `modules4`. Ne avrete bisogno se avete dei dispositivi

SCSI o USB oppure una scheda di rete o scheda PCMCIA e desiderate indirizzarla già durante l'installazione. Un dischetto dei moduli può essere utile quando volete utilizzare per esempio già durante l'installazione un determinato file system.

3.4.2 Creare un dischetto di boot con rawrite

Per creare il dischetto di avvio e dei moduli si ricorre al programma DOS `rawrite.exe` (CD 1, directory `dosutils\rawrite`. Serve chiaramente un sistema con DOS (ad es. FreeDOS) o Windows.

Ecco i passi da seguire se lavorate con Windows XP:

1. Inserite il CD 1 di SUSE LINUX.
2. Aprite una finestra di DOS (nel menù di avvio, su 'Programmi' → 'MS-DOS-Prompt').
3. Lanciate il programma rawrite.exe, indicando il percorso corretto del lettore del CD. Nell'esempio seguente, vi trovate sul disco `C:`, nella directory `Windows` ed il vostro lettore è contrassegnato dalla lettera `D:`

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

4. Dopo l'avvio, il programma vi chiede la fonte (ingl. source) e la destinazione (ingl. destination) del file da copiare. In questo esempio, si tratta del dischetto di caricamento appartenente al set di CD, la cui immagine si trova sul CD 1, sotto la directory `boot`. Il file si chiama semplicemente `bootdisk`. Non dimenticate di indicare il percorso per il vostro lettore di CD

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

   Enter source file name: d:\boot\bootdisk
   Enter destination drive: a:
   ```

Dopo aver indicato il lettore di destinazione `a:`, il programma rawrite vi invita ad inserire un dischetto formattato e a premere il tasto (Invio). Verrà visualizzata la progressione del processo di copiatura dei dati verrà visualizzato. Per interromperlo, premete la combinazione di tasti (Ctrl)-(C).

3.4.3 Creare i dischetti di avvio in un sistema Unix-like

Disponete di un sistema di tipo Unix o di un sistema Linux con un lettore CD-ROM funzionante e vi serve un dischetto formattato. Seguite questa procedura per creare un dischetto di avvio:

1. Se dovete ancora formattare il dischetto:

   ```
   fdformat /dev/fd0u1440
   ```

   Con questo comando verifica anche se il dischetto è esente da errori. Non proseguite se il mezzo presenta degli errori.

2. Inserite il CD 1 nel vostro lettore CD-Rom ed entrate nella directory `boot` sul CD: Con la versione attuale SUSE non è più necessario eseguire il mount del CD.

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

3. Ora create il dischetto di avvio con

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

4. Ripetete la procedura con le immagini `bootdsk2` e `bootdsk3`.

Il file `LEGGIMI` ovvero `README` nella directory `boot`, vi dà modo di approfondire la tematica delle immagini di dischetti; questi file possono essere visualizzati con `more` o `less`.

In questo modo potete creare anche le altre immagini di dischetti `modules1`, `modules2`, `modules3` e `modules4`. Ne avrete bisogno se avete dei dispositivi SCSI o USB oppure una scheda di rete o scheda PCMCIA e desiderate di indirizzarla già durante l'installazione. Un dischetto dei moduli può essere utile quando volete utilizzare per esempio già durante l'installazione un determinato file system.

Creare un dischetto dei moduli non una cosa triviale, per una descrizione del modo di generare un dischetto del genere consultate `/usr/share/doc/packages/yast2-installation/vendor.html`.

3.4.4 Avvio dal dischetto (SYSLINUX)

Il cosiddetto dischetto di avvio viene usato in circostanze particolari durante l'installazione (ad esempio, quando il PC non dispone di un lettore di CD-ROM). Il processo di boot viene inizializzato dal boot loader SYSLINUX (pacchetto `syslinux`). SYSLINUX è configurato in modo tale da non eseguire un rilevamento completo dell'hardware durante l'avvio. Essenzialmente, esso esegue i seguenti processi:

1. Controlla se il BIOS offre supporto per il framebuffer secondo lo standard VESA 2.0 e carica di conseguenza il kernel.
2. Legge i dati del monitor (informazioni DDC).
3. Legge il primo blocco del primo disco rigido (l'MBR), per poter assegnare, quando si effettuerà la configurazione del boot loader, gli ID del BIOS ai nomi dei dispositivi Linux. Il programma cercherà di leggere il blocco attraverso le funzioni lba32 del BIOS, per vedere se il BIOS supporti tali funzioni.

Suggerimento

Premendo (Shift) all'avvio di SYSLINUX, tutti questi processi verranno saltati. Per il debug, aggiungete la riga

```
verbose 1
```

in `syslinux.cfg`, e il boot loader vi comunicherà quale azione sta eseguendo.

Suggerimento

Se il PC non carica il sistema dal dischetto, probabilmente avrete bisogno di modificare la sequenza di caricamento nel BIOS ed impostarla su `A,C,CDROM`.

► **x86**
Su sistemi potete eseguire l'avvio anche con il CD 2; la differenza rispetto al CD 1, il quale utilizza un'immagine ISO atta al boot, è che il CD 2 viene avviato tramite un'immagine di dischetto di 2,88 Mbyte. Usate il CD 2 quando siete sicuri di poter eseguire il boot da CD, ma che fallisce con il CD 1 (soluzione fallback, ovvero di ripiego). ◄

3.4.5 Linux supporta il mio lettore di CD-Rom?

In generale, si può dire che la maggioranza dei lettori di CD-ROM viene supportata. In caso di difficoltà durante il boot dal lettore di CD-Rom, provate con il CD 2.

Se il sistema non supporta né CD-Rom né dischetti, sussiste la possibilità di utilizzare un lettore di CD-Rom esterno, connesso tramite USB, FireWire o SCSI per l'avvio del sistema. Spesso il tutto dipende dall'interazione tra BIOS ed hardware utilizzato. A volte un aggiornamento del BIOS risolve ogni difficoltà.

3.4.6 Installazione da una origine di rete

A volte non è data la possibilità di eseguire l'installazione utilizzando un lettore di CD-Rom, per svariate ragioni: il vostro lettore non viene supportato perché si tratta di un modello proprietario un po' datato, oppure perché il vostro portatile non dispone di un lettore di CD-Rom ma offre un adattore ethernet. SUSE LINUX permette di eseguire l'installazione in svariati modi su macchine sprovviste di lettore di CD-Rom ricorrendo a fonti disponibili sulla rete. Di solito in questi casi si ricorre a NFS o FTP via ethernet.

Questo approccio di installazione non è contemplato nel nostro servizio di supporto all'installazione gratuito, quindi la procedura riportata di seguito si rivolge in prima linea a utenti con un certo bagaglio di esperienza.

L'installazione di SUSE LINUX da un'origine sulla rete si suddivide in due fasi:

1. I dati richiesti ai fini dell'installazione (CD, DVD) devono essere resi disponibili su una macchina che fungerà da origine di installazione.
2. Il sistema da installare deve essere avviato dal dischetto, CD o dalla rete e bisogna eseguire le impostazioni di rete del caso.

Le fonti di installazione possono essere rese disponibili tramite una serie di protocolli di rete, come NFS FTP. Si veda la sezione 3.1.1 a pagina 88 per maggiori dettagli.

3.5 Nomi di dispositivo permanenti per i dispositivi SCSI

Dispositivi SCSI come ad esempio partizioni di hard disk ricevono all'avvio del sistema dei nomi di dispositivo assegnati più o meno dinamicamente. Questo non rappresenta un problema finché non si cambia nulla nella configurazione dei dispositivi e nel loro numero, se però si aggiunge un hard disk SCSI che viene rilevato dal kernel prima del vecchio hard disk, allora il vecchio disco riceve un nuovo nome e i nomi nella tabella di mount `/etc/fstab` non collimano più.

Per evitare difficoltà dovute a questa ragione, si dovrebbe utilizzare `boot.scsidev`. Questo script può essere abilitato tramite il comando `/sbin/insserv` e i parametri di boot necessari vengono archiviati sotto `/etc/sysconfig/scsidev`. Lo script `/etc/rc.d/boot.scsidev` imposta quindi nomi di dispositivo permanenti nella directory `/dev/scsi/`. Questi nomi di dispositivo possono essere utilizzati nel file `/etc/fstab`. Se volete dei nomi di dispositivo persistenti, potete definirli nel file `/etc/scsi.alias`; cfr. `man scsidev`.

Suggerimento

Nomi di dispositivo e udev

SUSE LINUX Enterprise Server continua a supportare boot.scsidev. Per SUSE LINUX si consiglia comunque, quando intendete creare nomi di dispositivo persistenti, di ricorrere ad udev. udev provvederà alle immissioni da effettuare in `/dev/by-id/`.

Suggerimento

Nel modo per esperti dell'editor dei runlevel, `boot.scsidev` va abilitato per il livello `B` per avere i riferimenti necessari in `/etc/init.d/boot.d`, in modo da potere creare i nomi durante il processo di avvio.

3.6 Configurazione dell'LVM

In questa sezione illustriamo i principi alla base di LVM e le sue caratteristiche principali che lo rendono così versatile. Nella sezione 3.6.2 a pagina 101 vi mostriamo come impostare LVM servendovi di YaST.

Avvertimento

Anche con LVM può verificarsi una perdita di dati, in caso di crollo di una applicazione, mancanza di corrente e comandi errati. Salvate i vostri dati prima di implementare LVM o riconfigurare dei volumi. Una copia di sicurezza è e rimane un accorgimento indispensabile.

Avvertimento

3.6.1 Il Logical Volume Manager

LVM (Logical Volume Manager) permette di distribuire lo spazio di dischi rigidi su diversi file system, cosa che si rivela essere utile soprattutto in quei casi in cui si presenta la necessità di dover modificare la segmentazione del disco rigido, dopo aver eseguito il partizionamento in fase di installazione. E visto che è accompagnato da una serie di difficoltà modificare il partizionamento con il sistema in esecuzione è stato ideato LVM che mette a disposizione un pool virtuale (volume group, abbreviato con VG) di memoria per creare dei logical volumes (LV) richiesti. Il sistema operativo indirizza questi LV al posto di partizioni fisiche. I volume group (VG), che chiameremo gruppi di volume possono includere più di un disco rigido, quindi un VG può essere costituito da diversi dischi o parti di essi. In tal modo LVM si svincola dallo spazio fisico del disco rigido per poter cambiarne segmentazione in modo più semplice e sicuro rispetto alla ripartizionamento fisico. Per maggiori dettagli sul partizionamento fisico si veda la sezione Tipi di partizioni a pagina 11 e la sezione 2.7.5 a pagina 73.

La figura 3.1 nella pagina seguente mette a confronto il partizionamento fisico (sulla sinistra) e la segmentazione LVM (sulla destra). Sulla sinistra, un singolo disco rigido è stato partizionato e presenta tre partizioni fisiche (PART), ognuna con un punto di mount (MP), in modo che il sistema operativo possa accedervi. Sulla destra, due dischi rigidi presentano due e tre partizioni fisiche. Vi sono stati definiti due gruppi di volume LVM (VG 1 e VG 2). VG 1 contiene due partizioni del DISK 1 ed una del DISK 2. VG 2 contiene le rimanenti due partizioni del DISK 2. Sotto LVM, le partizioni fisiche integrate in un gruppo di volume vengono chiamate volumi fisici (PV). All'interno dei gruppi di volume, sono stati definiti quattro logical volumes (LV 1 - LV 4), indirizzabili per il sistema operativo tramite i relativi punti di mount. Non è necessario allineare il limite tra diversi logical volume con il limite di una partizioni qualisasi. Si veda a riguardo LV 1 e LV 2 nel nostro esempio.

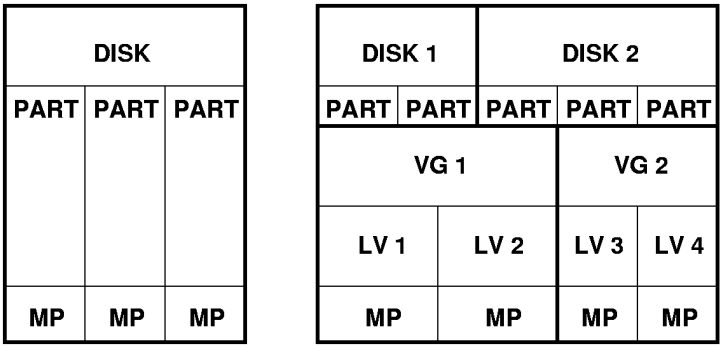

Figura 3.1: *Partizionamento fisico vs. LVM*

Caratteristiche di LVM:

- Più dischi rigidi/partizioni possono essere riuniti in un unica grande logical volume.
- Se un LV si riempie (p.es. `/usr`), potete espanderlo, in presenza della configurazione adeguata.
- Con l'LVM, potrete espandere dischi rigidi o LV addirittura con il sistema in esecuzione, a condizione che disponiate di hardware "hot-swapable", l'unico adatto a questo tipo di operazioni.
- Sussiste di abilitare il modo "striping" che distribuisce il flusso di dati di un logical volume su diversi PV. Se questi PV risiedono su diversi dischi rigidi si hanno migliori prestazioni per quel che riguarda l'acceso in lettura e scrittura, proprio come con RAID 0.
- Il feature "snapshot" consente, soprattutto con server, di ottenere dei backup consistenti con il sistema in esecuzione.

L'impiego dell'LVM si rivelerà vantaggioso anche su un PC domestico usato in modo intensivo e su piccoli server. Se contate di dover amministrare una quantità di dati sempre crescente, ad esempio, banche dati, archivi MP3 o directory di utenti, il Logical Volume Manager potrebbe tornarvi molto utile. Un LVM vi permette, per esempio, di creare file system più grandi del disco fisico. Un altro

vantaggio dell'LVM è che si possono creare fino a 256 volumi logici. Tenete comunque presente che lavorare con LVM differisce notevolmente dall'uso delle partizioni convenzionali. Per maggiori informazioni ed un'introduzione alla configurazione del "Logical Volume Manager" (LVM), consultate l'howto LVM ufficiale reperibile all'indirizzo `http://tldp.org/HOWTO/LVM-HOWTO/`.

A partire dal Kernel 2.6, vi è la versione 2 di LVM, compatibile verso il basso, ossia con la precedente versione di LVM, e permette di continuare a gestire vecchi gruppi di volume. Quando create dei nuovi gruppi di volume, stabilite se impiegare la nuova versione o la versione compatibile verso il basso. LVM 2 non necessità di alcun kernel patch, ricorre a dei device mapper integrati nel Kernel 2.6. Tale versione del Kernel supporta solo la versione 2 di LVM. In questa sezione quando si parla di LVM, si intende la versione 2 di LVM.

3.6.2 Configurazione di LVM tramite YaST

Il partizionatore per esperti di YaST è uno strumento professionale per eliminare o creare delle partizioni create per essere utilizzate con LVM. Per creare una partizione LVM cliccate su 'Crea' → 'Non formattare' e quindi su '0x8e Linux LVM' quale ID della partizione. Dopo aver creato tutte le partizioni da utilizzare con LVM, cliccate su 'LVM' per avviare il processo configurativo.

Creare dei gruppi di volume

Se ancora non vi è alcun gruppo di volume sul vostro sistema, createne uno (si veda la figura 3.2 nella pagina successiva). Potete creare dei gruppi aggiuntivi tramite 'Aggiungi gruppo', comunque basta un solo gruppo di volume; `system` è il nome suggerito per il gruppo di volume che conterrà i file di sistema di SUSE LINUX. La dimensione fisica determina la dimensione del blocco fisico del gruppo di volume. In un gruppo di volume lo spazio viene gestito in base questa dimensione. Tale valore verrà normalmente fissato su 4 megabyte, consentendo un'estensione massima di 256 gigabyte per volumi fisici e logici. La dimensione fisica va aumentata (p.es. a 8, 16 o 32 megabyte) solo se avete bisogno di un volume logico più grande di 256 megabyte.

Configurare PV (Physical Volume)

Dopo aver creato il gruppo di volume, nel seguente dialogo verranno elencate tutte le partizioni che presentino l'indicazione "Linux LVM" o "Linux native". Tutte le partizioni swap e DOS non verranno pertanto incluse nella lista. Se una

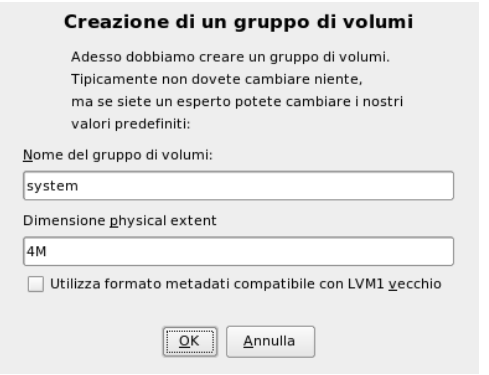

Figura 3.2: *Creare un gruppo di volumi*

partizione è già stata assegnata ad un gruppo di volume, il nome di quest'ultimo verrà riportato nella lista. Partizioni non allocate saranno contrassegnate con un "--".

Il gruppo di volume da elaborare può essere determinato nel box delle selezioni che si trova in alto a sinistra. Con i bottoni in alto a destra, potrete creare nuovi gruppi di volume e cancellarne dei vecchi. Tuttavia, sarà possibile eliminare solo gruppi di volume ai quali non è più attribuita alcuna partizione. Una partizione assegnata ad un gruppo di volume anche chiamata Physical Volume (abbr.: PV).

Per aggiungere una partizione ancora non allocata al gruppo di volume selezionato, cliccate sulla partizione e quindi su 'Aggiungi volume'. A questo punto, il nome del gruppo di volume verrà riportato nella partizione selezionata. Vi consigliamo di assegnare tutte le partizioni di un LVM ad un gruppo di volume, se non volete lasciare inutilizzato parte dello spazio della partizione. Prima di lasciare questa finestra attribuite ad ogni gruppo di volume almeno un volume fisico. Proseguite con 'Prossimo'.

Configurare i volumi logici

Tramite 'Aggiungi' si apre una menu in cui immettere i vostri dati per creare un nuovo volume logico, cioé la dimensione, file system e punto di mount. Di solito viene creato un file system, ad es. reiserfs o ext2, su un volume logico e quindi assegnato un punto di mount. I file archiviati sul volume logico possono essere

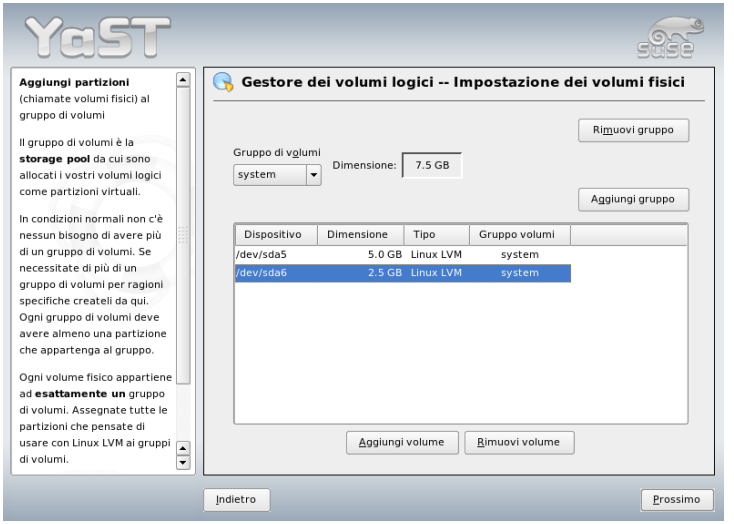

Figura 3.3: *Impostare PV*

inidirizzati tramite questo punto di mount. Inoltre, è possibile distribuire il flusso di dati nel volume logico tra diversi volumi fisici (striping). Se i volumi fisici risiedono su diversi dischi rigidi si realizzano dei benefici per quanto riguarda le prestazioni in scrittura e lettura (alla stregua di RAID 0). C'è comunque da tenere presente che lo striping di LV con n stripe può essere creato in modo corretto solo se lo spazio di memoria richiesto dall'LV si lascia allocare uniformemente ai n volumi fisici. Se chiaramente vi sono solo due PV, non è possibile avere un LV con tre stripe.

Avvertimento

Striping

YaST a questo punto non è in grado di determinare la correttezza delle vostre immissioni riguardanti lo striping. Gli errori verranno a galla solo dopo aver implementato LVM.

Avvertimento

Normalmente, su un volume logico viene creato un file system (p.es. reiserfs, ext2), al quale viene poi attribuito un punto di mount. Sotto questo punto di

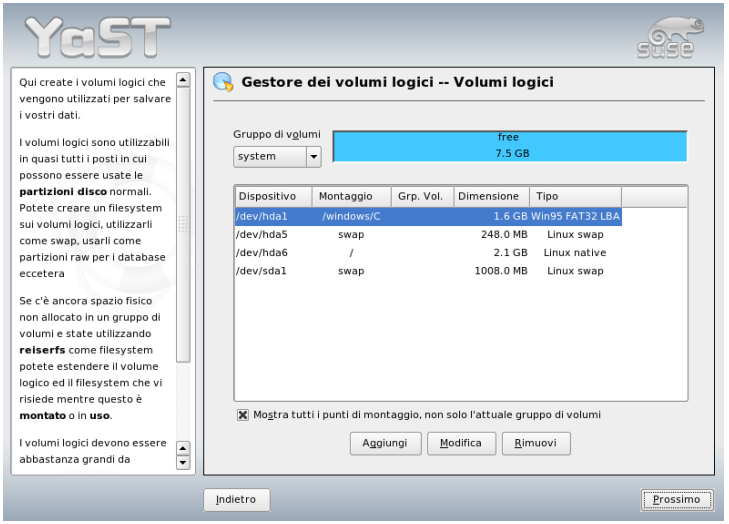

Figura 3.4: *Amministrare i volumi logici*

mount, nei sistemi installati, si trovano i file memorizzati su questo logical volume. Nella lista, sono riportate tutte le normali partizioni Linux, con un punto di mount, nonché tutte le partizioni swap ed i volumi logici esistenti.

In caso abbiate configurato già in precedenza un LVM nel vostro sistema, i volumi logici esistenti saranno riportati qui. Vi resta, tuttavia, da attribuire a questi volumi logici il punto di mount adatto. Se impostate per la prima volta degli LVM su di un sistema, in questa maschera non sarà riportato ancora alcun volume logico: dovrete crearne uno per ogni punto di mount (tramite il bottone 'Aggiungere') e determinarne l'estensione, il tipo di file system (p.es. reiserfs oppure ext2) ed il punto di mount (p. es. `/var`, `/usr`, `/home`).

Se avete già configurato LVM sul vostro sistema, potete immettere ora i volumi logici. Prima di proseguire, assegnate i punti di mount a questi volumi logici. 'Prossimo' vi riporta nel partizionatore per esperti di YaST, dove potete terminare le vostre impostazioni.

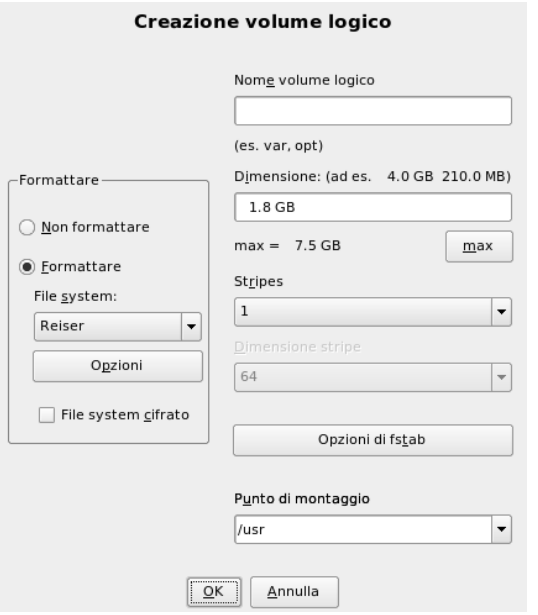

Figura 3.5: *Creare volumi logici*

Amministrazione diretta di LVM

Se avete già configurato LVM e volete solo modificare qualcosa, vi è anche l'opzione di ricorrere al centro di controllo di YaST per apportare le vostre modifiche; selezionate in questo caso 'Sistema' → 'LVM'. In linea di massima questa finestra vi consente di eseguire le operazioni descritte sopra, fatta eccezione per il partizionamento fisico. I volumi fisici e logici vengono mostrati in due elenchi e potrete amministrare il vostro sistema LVM applicando quanto descritto fin qui.

3.7 Configurazione di Soft-RAID

RAID (ingl. Redundant Array of Inexpensive Disks) permette di combinare più partizioni in un unico grande disco rigido *virtuale*, con lo scopo di ottimizzare la prestazione del sistema e la sicurezza dei dati. Tuttavia, l'una è a spese dell'altra.

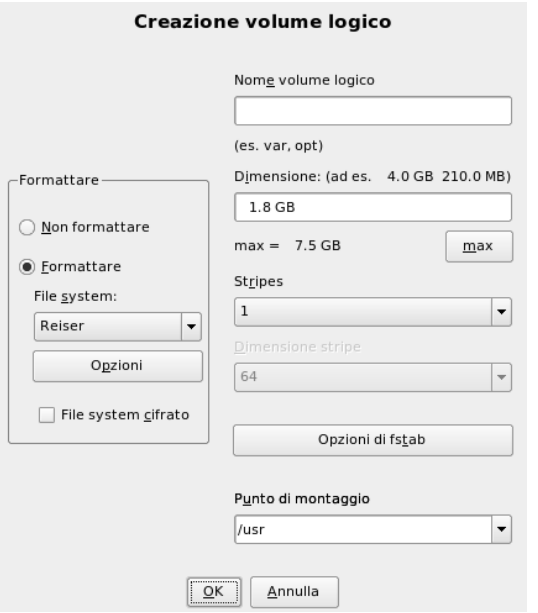

Figura 3.6: *Creare volumi logici*

La maggior parte degli controller RAID utilizzano il protocollo SCSI perché permette di indirizzare un vasto numero di dischi rigidi in un modo più efficace del protocollo IDE ed è inoltre più adatto per l'elaborazione parallela di comandi. Vi sono alcuni controller RAID che supportano dischi rigidi IDE o SATA. Consultate a riguardo la banca dati hardware all'indirizzo `http://cdb.suse.de`.

3.7.1 Soft RAID

Al posto di un controllore RAID, molto costoso, si può ricorrere anche ad un Soft-RAID. SUSE LINUX vi offre la possibilità di riunire, con YaST, dischi diversi in un unico sistema Soft-RAID, un'alternativa più economica all' hardware RAID. RAID prevede diverse possibilità, presentando ognuna propri vantaggi e caratteristiche, per combinare diversi dischi rigidi in un sistema RAID, a secondo delle scopo che si persegue. Con l'espressione *livelli RAID* si indicano i vari modi di realizzare quanto descritto finora.

Livelli di RAID diffusi

RAID 0 Questo livello migliora la prestazione sotto il punto di vista dell' accesso ai vostri dati. In fondo, non si tratta di RAID, dal momento che non vi è un backup dei dati, ma si usa ormai definirlo così. In un sistema *RAID 0*, si raggruppano almeno due dischi rigidi. Le prestazioni sono molto buone, con un unico difetto: se anche uno solo dei vostri non importa quanti dischi rigidi dovesse venire a mancare, il sistema RAID è inutilizzabile ed i vostri dati saranno persi.

RAID 1 Questo livello vi offre una sicurezza dei dati estremamente soddisfacente, dal momento che i vostri dati vengono copiati in un rapporto di 1:1 su di un altro disco rigido. Questo procedimento viene chiamato *specchiamento dei dischi rigidi*: se uno dei dischi viene danneggiato, disporrete di una copia esatta del suo contenuto su un altro disco. Teoricamente, potreste perdere tutti dischi tranne uno senza dover rinunciare ai vostri dati. Con un RAID 1 (più lento del 10-20 %), le prestazioni in termini di scrittura risentono dello specchiamento. In compenso, la lettura è molto più veloce rispetto ad un unico disco rigido fisico, perché i dati sono presenti in duplice copia e quindi leggibili parallelamente. In generale si può affermare che il livello 1 offre una velocità di lettura doppia rispetto ad un disco singolo e quasi la stessa velocità di scrittura.

RAID 2 e RAID 3 Si tratta di implementazioni RAID atipici. Il livello 2 tratta i dati a livello dei bit piuttosto che a livello di blocco. Il livello 3 esegue lo striping a livello dei byte con un disco di parità dedicato e non è in grado di elaborare richieste simultanee. Entrambi questi livelli non sono molto diffusi.

RAID 4 Il livello 4 esegue lo striping a livello di blocco come il livello 0 ed offre inoltre un disco di parità dedicato. Se viene a mancare un disco, il disco di parità viene utilizzato ai fini di un ripristino. Il disco di parità comunque rallenta considervolmente l'accesso in scrittura. Nonostante ciò il livello 4 viene utilizzato da alcuni.

RAID 5 RAID 5 rappresenta un compromesso ottimizzato tra i livelli 0 e 1 per quel che riguarda prestazioni e ridondanza. Il numero massimo dei dischi rigidi utilizzabili corrisponde al numero dei dischi impiegati meno uno. I dati vengono distribuiti tra i dischi come sotto RAID 0. Alla sicurezza ci pensano i *blocchi di parità*, che, con RAID 5, vengono costruiti su una delle partizioni e collegati con XOR (OR esclusivo) l'uno all'altro: in questo modo, in caso di perdita di una partizione, è possibile ricostruirne il contenuto

in base a XOR, tramite il corrispondente blocco di parità. Tuttavia, nel caso di RAID 5, non vi potrà essere più di un disco alla volta ad essere danneggiato: se un disco risulta essere danneggiato, deve essere immediatamente sostituito, affinché non vadano persi dei dati.

Altri livelli RAID Sono stati sviluppati anche altri livelli RAID (RAIDn, RAID 10, RAID 0+1, RAID 30, RAID 50, etc.), in alcuni casi si tratta di implementazioni proprietarie messe a punto da produttori di hardware. Si tratta di livelli poco diffusi, per tale ragione non entreremo nei dettagli.

3.7.2 Configurazione di Soft-RAID con YaST

Per la configurazione di Soft-RAID potete ricorrere al partizionatore per esperti di YaST (si veda la sezione 2.7.5 a pagina 73). Questo strumento per il partizionamento professionale permette di modificare e cancellare delle partizioni esistenti e di crearne delle nuove da utilizzare con Soft-RAID. Per creare delle partizioni RAID cliccate su 'Crea' → 'Non formattare' e selezionate quindi '0xFD Linux RAID' quale ID della partizione. Per RAID 0 e RAID 1, sono almeno due le partizioni richieste — per RAID 1 sono richieste esattamente due. Se usate invece RAID 5 sono richieste almeno tre partizioni. Vi consigliamo di scegliere solo partizioni delle stesse dimensioni. Le singole partizioni di un RAID dovrebbero essere situate su dischi rigidi diversi, in modo da eliminare il rischio di perdita di dati a causa di un disco difettoso (nel caso di RAID 1 e 5) nonché per ottimizzare la performance di RAID 0. Dopo aver concluso con la creazione delle partizioni da utilizzare con RAID, cliccate su 'RAID' → 'Crea RAID' per iniziare con la configurazione RAID.

Nella prossima finestra selezionate il livello RAID (0, 1, e 5); si veda la sezione 3.7.1 a pagina 106 per maggiori dettagli). Dopo aver cliccato su 'Prossimo' avrete un elenco con tutte le partizioni di tipo "Linux RAID" o "Linux native" (si veda la figura 3.7 a fronte). L'elenco non include partizioni swap e DOS. Se una partizione è stata già assegnata ad un volume RAID, viene indicato nell'elenco il nome del dispositivo RAID (p. es., `/dev/md0`). Le partizioni non allocate presentano un "--".

Per aggiungere una partizione che non è stata ancora assegnata al volume RAID selezionato, cliccate innanzitutto sulla partizione e quindi su 'Aggiungi'. In tal modo, il nome del dispositivo RAID viene immesso accanto alla partizione selezionata. Dovete allocare ogni partizione riservata per RAID, altrimenti lo spazio sulla partizione rimane inutilizzato. Dopo aver assegnato tutte le partizioni, cliccate su 'Prossimo' per proseguire nell'iter configurativo e cesellare il livello delle prestazione (si veda la figura 3.8 a pagina 110).

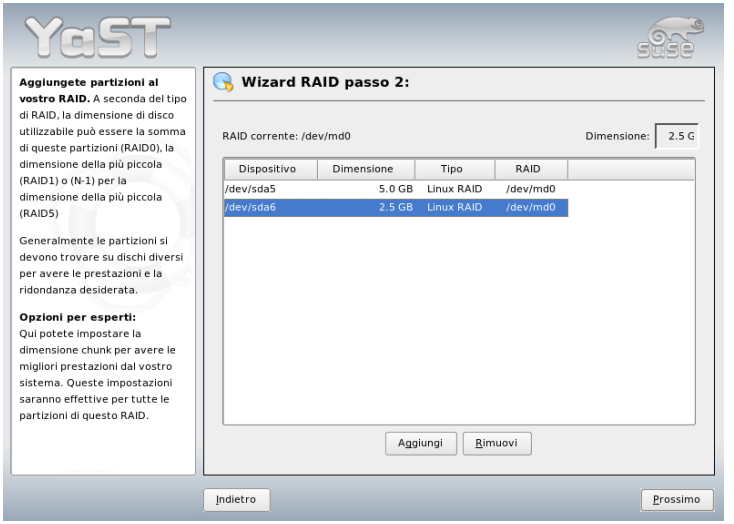

Figura 3.7: *Partizioni RAID*

Come per la procedura di partizionamento consueta, impostate il file system, modo di cifratura e punto di mount per il volume RAID. Selezionando 'Superblocco persistente' le partizioni RAID vengono rilevate come tali al boot. Dopo aver portato a termine la configurazione con 'Fine' `/dev/md0` ed altri dispositivi saranno contrassegnati con *RAID*.

3.7.3 Troubleshooting

Se una partizione RAID è corrotta, ve lo indica il contenuto del file `/proc/mdstats`. In linea di massima, in caso di guasto, chiudete il vostro sistema Linux e sostituite il disco difettoso con un nuovo disco partizionato in modo identico. Quindi rilanciate il vostro sistema e date il comando `mdadm /dev/mdX --add /dev/sdX` per integrare in modo automatico il nuovo disco nel sistema RAID e ricostruirlo altresì in modo automatico. Chiaramente al posto di 'X' dovete indicare il vostro ID di dispositivo.

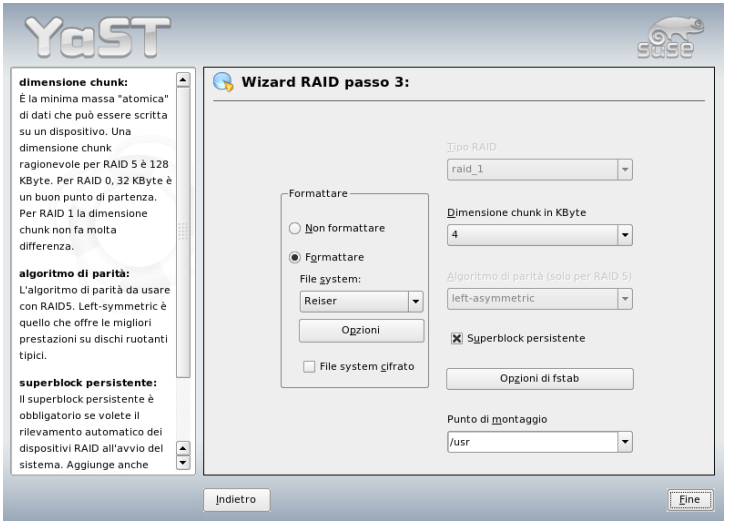

Figura 3.8: *Impostazione del file system*

3.7.4 Ulteriori informazioni

Per una guida alla configurazione di Soft-RAID ed altri dettagli, consultate gli Howto riportati:

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

Vi sono anche delle mailing list per RAID Linux p.es.: `http://www.mail-archive.com/linux-raid@vger.rutgers.edu`

4

Aggiornare il sistema e amministrare i pacchetti

SUSE LINUX vi offre la possibilità di aggiornare un sistema, senza doverlo reinstallare. E' possibile sia *attualizzare singoli pacchetti di software* che *attualizzare l'intero sistema*. I singoli pacchetti possono essere anche installati con il programma di gestione dei pacchetti rpm.

4.1 Aggiornare SUSE LINUX

É un fenomeno noto: il software cresce da versione a versione! É perciò consigliabile controllare tramite il comando `df`, *prima* dell'aggiornamento, com'è sfruttato lo spazio sulle partizioni. Se avete l'impressione di non avere molto spazio, eseguite un backup dei dati e ripartizionate il sistema. Non esiste un criterio universale che stabilire come suddividere lo spazio disponibile: tutto dipende dal tipo di partizione esistente, dal software selezionato e dalla versione da aggiornare alla nuova versione di SUSE LINUX.

4.1.1 Preparazione

Prima di iniziare l'aggiornamento, i vecchi file di configurazione dovrebbero essere copiati su un dispositivo a parte (streamer, hard disk estraibile, CD-Rom, dispositivo ZIP). Principalmente si tratta dei file contenuti in `/etc`; controllate inoltre i file di configurazione sotto `/var` nonché `/opt`. Inoltre è sempre bene scrivere sul supporto di backup anche i dati attuali che risiedono sotto `/home` (le directory `HOME`) dell'utente. Il backup dei dati va eseguito come amministratore di sistema `root`; solo `root` ha i permessi di leggere tutti i file locali.

Prima di iniziare un aggiornamento annotatevi la partizione root; il comando `df /` vi indica il nome del dispositivo della vostra partizione root; nel caso dell'esempio 4.1 in questa pagina è `/dev/hda2` (montata sotto `/`) la partizione root da annotare.

Esempio 4.1: *Panoramica con* `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 Problemi possibili

Controllare passwd e group in /etc

Prima di un update va assicurato che `/etc/passwd` e `/etc/group` non presentano degli errori di sintassi. A tal scopo invocate come `root` i programmi di verifica `pwck` e `grpck` ed eliminate gli errori rilevati.

PostgreSQL

Prima di eseguire un update di PostgreSQL (`postgres`), consigliamo di fare un dump delle banche dati; cfr. la pagina di manuale di `pg_dump`. Ne avrete naturalmente bisogno solo se avete effettivamente usato PostgreSQL prima di aggiornarlo.

4.1.3 L'update con YaST

Dopo i preparativi riportati nella sezione 4.1.1 nella pagina precedente avviate il sistema.

1. Avviate il sistema come per l'installazione (si veda la sezione 1.1 a pagina 4. In YaST dopo aver selezionato la lingua, *non* selezionate 'Nuova installazione' ma 'Update del sistema esistente'.
2. YaST controlla se vi sono più di una partizione root; in caso negativo prosegue. Se vi sono più partizioni del genere, selezionate quella giusta e confermate la vostra selezione con 'Prossimo' (nell'esempio nella sezione 4.1.1 nella pagina precedente avevate annotato `/dev/hda2`). YaST leggerà il vecchio `fstab` che si trova su questa partizione, analizza e monta i file system lì registrati.
3. In seguito vi è la possibilità di creare una copia di sicurezza dei file di sistema durante l'aggiornamento. Questa opzione rallenta il processo di aggiornamento, ma dovrebbe essere selezionata se non disponete di un backup del sistema recente.
4. Nel prossimo dialogo potete stabilire se aggiornare solo software già installato oppure aggiungere nuovi ed importanti componenti di software al sistema (modo upgrade). Si consiglia di accettare quanto proposto (p.es. 'Sistema standard'). Delle eventuali incongruenze possono essere eliminate in un secondo momento ricorrendo a YaST.

4.1.4 Aggiornare singoli pacchetti

Oltre all'update completo, potete naturalmente aggiornare anche singoli pacchetti; in questo caso dovete *voi stessi* fare attenzione affinché il sistema rimanga consistente: per dei consigli rimandiamo all'URL: `http://www.novell.com/linux/download/updates/`

Nella selezione dei pacchetti di YaST avete mano libera. Se scegliete di aggiornare un pacchetto fondamentale per il funzionamento del sistema, YaST vi avviserà: tali pacchetti dovrebbero venire aggiornati nel modo speciale di update. Molti pacchetti contengono per esempio *librerie condivise* probabilmente utilizzate dai processi in esecuzione al momento dell'aggiornamento stesso. Un aggiornamento con il sistema in esecuzione potrebbe causare dei malfunzionamenti.

4.2 Da versione a versione

Nelle sezioni successive elenchiamo quali aspetti sono cambiati da una versione all'altra. In questo sommario vi informiamo per esempio se sono state modificate delle impostazioni fondamentali o se sono stati spostati dei file di configurazione oppure se sono stati modificati dei noti programmi. Attireremo la vostra attenzione solo su quelle cose rilevanti per il lavoro quotidiano dell'utente o dell'amministratore di sistema.

Appena rilevati, le difficoltà e le particolarità della rispettiva versione verranno pubblicati sul server web; cfr. i link riportati di seguito. Per importanti aggiornamenti di singoli pacchetti, visitate il sito `http://www.novell.com/products/linuxprofessional/downloads/` e utilizzate la funzionalità di aggiornamento in linea di YaST (YOU che sta per YaST Online Update); si veda la sezione 2.2.3 a pagina 49.

4.2.1 Dalla versione 8.1 alla 8.2

Problemi e particolarità: `http://portal.suse.com/sdb/en/2003/04/bugs82.html`

- Supporto 3D per schede grafiche nVidia (cambiamenti): gli rpm `NVIDIA_GLX/NVIDIA_kernel` (e lo script `switch2nvidia_glx`) non sono più inclusi. Scaricate l'installer nVidia per `Linux IA32` dal sito web di nVidia (`http://www.nvidia.com`), installate con esso il driver e abilitate il supporto 3D con SaX2 o YaST.
- Quando eseguite una nuova installazione viene installato xinetd al posto di inetd e configurato con valori sicuri; si veda la directory `/etc/xinetd.d`). Se aggiornate il sistema, inetd rimane.

- PostgreSQL si presenta nella versione 7.3. Se aggiornate da una versione 7.2.x dovete eseguire un *dump/restore* con `pg_dump`. Se la vostra applicazione analizza i cataloghi di sistema è necessario apportare degli adattamenti, visto che con la versione 7.3 sono stati introdotti gli schemi. Per ulteriori informazioni visitate: `http://www.ca.postgresql.org/docs/momjian/upgrade_tips_7.3`.

- La versione 4 di stunnel non supporta più opzioni della riga di comando. Avete comunque lo script `/usr/sbin/stunnel3_wrapper` che converte le opzioni della riga di comando in un file di configurazione adatto per stunnel (al posto di `OPTIONS` immettete le vostre opzioni):

  ```
  /usr/sbin/stunnel3_wrapper stunnel OPTIONS
  ```

  Il file di configurazione così generato emette l'output su stdout (standard output) in modo da poter utilizzare queste informazioni per generare un file di configurazione permanente.

- openjade (`>openjade`) è il motore DSSSL che attualmente sostituisce jade (`jade_dsl`) quando invocate db2x.sh (`docbook-toys`). Per motivi di compatibilità i pacchetti sono disponibili anche senza il prefisso `o`.

  Se alcune applicazioni dipendono dalla directory `jade_dsl` e dei file finora ivi installati, eseguite gli adattamenti del caso basandovi su `/usr/share/sgml/openjade` oppure create un link come `root` eseguendo:

  ```
  cd /usr/share/sgml
  rm jade_dsl
  ln -s openjade jade_dsl
  ```

  Per evitare un conflitto con `rzsz`, il tool a riga di comando `sx` continua a chiamarsi `s2x` e rispettivamente `sgml2xml` oppure `osx`.

4.2.2 Dalla versione 8.2 alla 9.0

Problemi e particolarità: `http://portal.suse.com/sdb/en/2003/07/bugs90.html`

- E' ora disponibile la versione 4 del gestore dei pacchetti RPM. La funzionalità per compilare dei pacchetti è stata estrapolata in un programma a sé stante chiamato `rpmbuild`. `rpm` continua ad essere utilizzato in fase di installazione, per update e richieste indirizzate alla banca dati. Si veda la sezione 4.3 a pagina 130.

- Per quel che riguarda il processo di stampa vi è il pacchetto `footmatic-filters`. Il contenuto è stato preso da `cups-drivers`, visto che permette di stampare anche se CUPS non è installato. In tal modo è possibile eseguire delle impostazioni con YaST che non dipendono dal sistema di stampa (CUPS, LPRng). Questo pacchetto include iI file di configurazione `/etc/foomatic/filter.conf`.
- Se utilizzate LPRng/lpdfilter, adesso sono richiesti i pacchetti `footmatic-filters` e `cups-drivers`.
- Le risorse XML dei pacchetti software vengono rese accessibili tramite le registrazioni in `/etc/xml/suse-catalog.xml`. Questo file non può essere editato con `xmlcatalog`, altrimenti scompaiono i commenti richiesti per assicurare un aggiornamento corretto. `/etc/xml/suse-catalog.xml` viene reso accessibile tramite una istruzione `nextCatalog` in `/etc/xml/catalog`, in modo che tool XML- come `xmllint` oppure `xsltproc` - siano in grado di trovare automaticamente le risorse locali.

4.2.3 Dalla versione 9.0 alla 9.1

Rimandiamo all'articolo "Known Problems and Special Features in SUSE LINUX 9.1" disponibile non solo in inglese nella banca dati di supporto di SUSE all'indirizzo `http://portal.suse.com` che troverete immettendo la parola chiave *special features*. Per ogni versione di SUSE LINUX vi è un articolo del genere.

Passaggio al Kernel 2.6

SUSE LINUX si basa sulla versione del kernel 2.6; la versione precedente 2.4 non dovrebbe venire più utilizzata, visto che probabilmente i programmi forniti a corredo non funzioneranno con il Kernel 2.4. Inoltre va tenuto in considerazione quanto segue:

- Il processo di caricamento dei moduli adesso si configura tramite il file `/etc/modprobe.conf`; il file `/etc/modules.conf` diventa obsoleto. YaST cercherà di convertire il file (cfr. anche lo script `/sbin/generate-modprobe.conf`).
- I moduli hanno ora il suffisso `.ko`.
- Il modulo `ide-scsi` non serve più per masterizzare dei CD.

- Le opzioni dei moduli sonori di ALSA non hanno più il prefisso `snd_`.
- `sysfs` completa ora il file system `/proc`.
- E' stato ottimizzato il power management (in particolare ACPI) e adesso può essere impostato tramite un modulo di YaST.

Il mount di partizioni VFAT

Al mount di partizioni VFAT, il parametro `code` va modificato in `codepage`. Se il processo di mount di una partizione VFAT crea delle difficoltà, verificate se il file `/etc/fstab` contiene il vecchio nome parametro.

Standby e Suspend con ACPI

Con il nuovo Kernel 2.6 viene supportato lo Standby/Suspend con ACPI. Considerate che queste funzionalità si trovano ancora in uno stato sperimentale e che non vengono supportate da ogni componente hardware. Questa funzionalità richiede il pacchetto `powersave`. Per maggiori informazioni riguardanti questo pacchetto rimandiamo a `/usr/share/doc/packages/powersave`. Un front-end grafico è reperibile nel pacchetto `kpowersave`.

Dispositivi di immissione

Per quel che riguarda i dispositivi di immissione (*Input devices*) cfr. l'articolo riportato sopra "Known Problems and Special Features in SUSE LINUX 9.1" che trovate andando su `http://portal.suse.com` e utilizzando quale parola chiave nella vostra ricerca *special features*.

Native POSIX Thread Library e glibc 2.3.x

Programmi linkati a NGPT (*Next Generation POSIX Threading*) non girano con glibc 2.3.x. Tutti i programmi interessati da questa restrizione, non inclusi in SUSE LINUX devono essere ricompilati con linuxthreads o NPTL (*Native POSIX Thread Library*). La preferenza va data a NPTL, visto che si tratta dello standard di prossima generazione.

In caso di difficoltà con NPTL si può ripiegare su implementazioni antecenti di linuxthreads impostando la seguente variabile di ambiente (⟨*versionekernel*⟩ va sostituito con il numero di versione del rispettivo kernel):

```
LD_ASSUME_KERNEL=versionekernel
```

Ecco i numeri di versione possibili:

2.2.5 (i386, i586): linuxthreads senza floating stack

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

Indicazioni relative al kernel e linuxthreads con floating stack: programmi che utilizzano `errno`, `h_errno` e `_res` devono integrare i relativi file header (`errno.h`, `netdb.h` e `resolv.h`) tramite `#include`. Per programmi C++ con supporto multithread che utilizzano *thread cancellation*, la variabile di ambiente `LD_ASSUME_KERNEL=2.4.1` va impostata in modo da richiedere l'utilizzo della libreria linuxthreads.

Adattamenti per Native POSIX Thread Library

NPTL (*Native POSIX Thread Library*) in SUSE LINUX 9.1 è incluso come pacchetto thread. NPTL è stato sviluppato in modo binariamente compatibile (ingl. binary compatible) con le precedenti librerie linuxthreads. Dove però i linuxthreads non si attengono agli standard di POSIX, NPTL richiede degli adattamenti che nella fattispecie sono: trattamento dei segnali e `getpid` che ritorna lo stesso valore in tutti i thread; thread handler registrati con pthread_atfork non funzionano se si utilizza `vfork`.

Configurazione dell'interfaccia di rete

Il processo di configurazione di una interfaccia di rete è cambiato. Finora, dopo la configurazione di una interfaccia non presente veniva avviato il processo di inizializzazione dell'hardware. Ora viene eseguita una ricerca del nuovo hardware che viene subito inizializzato in modo da poter proseguire con la configurazione della nuova interfaccia.

Inoltre sono stati introdotti dei nuovi nomi per i file di configurazione. Dato che i nomi vengono generati dinamicamente e che l'uso di dispositivi hotplug si diffonde sempre di più, un nome del tipo `eth0`, `eth1`, etc. non e più adatto più ai fini della configurazione. Quindi si ricorre a descrizioni univoche come l'indirizzo MAC o lo slot PCI per la denominazione delle configurazioni delle interfacce. Chiaramente potrete utilizzare nomi di interfacce non appena compaiano. Comandi del tipo `ifup eth0` o `ifdown eth0` sono ancora consentiti.

La configurazione dei dispositivi si trova in `/etc/sysconfig/hardware`. Le interfacce messe a disposizione da questi dispositivi si trovano di solito (con nome diverso) in `/etc/sysconfig/network`. Si veda la descrizione dettagliata sotto `/usr/share/doc/packages/sysconfig/README`.

Configurazione dell'audio

Dopo un update vanno riconfigurate anche le schede audio. Potete utilizzare a tal fine il modulo audio di YaST, basta immettere il seguente comando come `root`: `yast2 sound`.

Top-Level-Domain .local come dominio link-local

La libreria resolver tratta i domini top-level `.local` come domini "link-local" ed invia richieste DNS multicast all'indirizzo multicast `224.0.0.251`, porta `5353`; si tratta di una modifica incompatibile. Se avete già un dominio `.local` nella configurazione del server dei nomi, si deve utilizzare un altro nome di dominio. Per ulteriori informazioni su DNS multicast consultate `http://www.multicastdns.org`.

UTF-8: la codifica del sistema

Di default si ha la codifica `UTF-8`. Durante l'installazione standard, si avrà un "locale" con `.UTF-8` quale codifica (*encoding*), cioé `it_IT.UTF-8`. Maggiori dettagli sono reperibili all'indirizzo `http://www.suse.de/~mfabian/suse-cjk/locales.html`

Convertire il nome file in UTF-8

File in file system che sono stati creati precedentemente non utilizzano (se non esplicitamente impostato) la codifica UTF-8 per nomi di file. Se questi file includono caratteri non ASCII verranno visualizzati in modo quasi "irriconoscibile". Per una correzione si può utilizzare lo script `convmv`, che converte la codifica dei nomi file in UTF-8.

Tool di shell compatibili con lo standard POSIX del 2001

Tool di shell in `coreutils` come `tail`, `chown`, `head`, `sort` etc. seguono di default lo standard POSIX del 2001 (*Single UNIX Specification, version 3 == IEEE Std 1003.1-2001 == ISO/IEC 9945:2002*) e non più lo standard del 1992. Il vecchio modo di reagire può essere forzato tramite una variabile di ambiente:

```
_POSIX2_VERSION=199209
```

Il nuovo valore è 200112 e si tratta del valore di default per `_POSIX2_VERSION`. E' possibile consultare lo standard SUS (gratuitamente, ma è richiesta la registrazione) all'indirizzo: `http://www.unix.org`

Tabella 4.1: Confronto POSIX 1992/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`

Suggerimento

Software di terzi probabilmente non si attiene ancora al nuovo standard; in questi casi è consigliabile impostare la variabile di ambiente come descritto sopra: `_POSIX2_VERSION=199209`.

Suggerimento

/etc/gshadow obsoleto

`/etc/gshadow` è stato rimosso, essendo diventato superfluo; ecco i motivi:

- non viene più supportato da parte della glibc.
- non vi è un'interfaccia ufficiale per questo file; neanche la suite di shadow ne offre una.
- la maggioranza dei tool che controllano la password di gruppo non supportano il file e lo ignorano per le ragioni appena menzionate.

OpenLDAP

Visto che è cambiato il formato della banca dati, le banche dati vanno ricreate. Durante un update si cerca di eseguire questa conversione in modo automatico; vi saranno però dei casi in cui ciò non produce il risultato atteso.

E' stata migliorata considerevolmente la verifica degli schemi. In tal modo non sarà più possibile eseguire alcuna operazione (non conforme allo standard), cosa invece possibile con la versione precedente del server LDAP.

La sintassi del file di configurazione è in parte cambiata dovuto anche alle ACL. Per maggiori informazioni sull'update consultate il seguente file ad installazione effettuata: `/usr/share/doc/packages/openldap2/README.update`

Sostituzione di Apache 1.3 con Apache 2

Il server web Apache (versione 1.3) è stato sostituito con Apache 2. Per la documentazione della versione 2.0 rimandiamo al seguente sito web `http://httpd.apache.org/docs-2.0/en/`. Un update di un sistema su cui girà un server HTTP cancellerà il vecchio pacchetto Apache ed installerà Apache 2. Si dovrà adattare il sistema tramite YaST o manualmente. I file di configurazione sotto `/etc/httpd` si troveranno adesso sotto `/etc/apache2`.

Ai fini dell'esecuzione contemporanea di diverse richieste si ha la scelta tra cosiddetti thread e processi. La gestione dei processi rappresenta un modulo a se stante, il cosiddetto multi-processing-module (MPM). Apache 2 richiede quindi il pacchetto `apache2-prefork` (consigliato per le sue doti in termini di stabilità) o `apache2-worker`. In base all'MPM, Apache 2 reagirà in modo diverso alle richieste. Questo influisce in prima linea sulla performance e sull'uso dei moduli. Queste caratteristiche vengono trattate in modo dettagliato nel sezione 30.4 a pagina 525.

Apache 2 supporta il protocollo Internet di prossima generazione IPv6.

Esiste adesso un meccanismo che permette ai produttori di moduli di determinare loro la sequenza di caricamento dei moduli, in modo che l'utente non dovrà più preoccuparsene. La sequenza nella quale vengono caricati i moduli rappresenta spesso un aspetto non trascurabile. Finora veniva stabilita una sequenza di caricamento. Ad esempio un modulo che permette solo agli utenti autenticati di accedere ad una determinata risorsa deve venir caricato come primo, in modo che la risorsa non risulti neanche visibile agli utenti sprovvisti del permesso di accedervi.

Sussiste la possibilità di applicare un filtro alle richieste rivolte a Apache e alle rispettive risposte.

Da samba~2.x a samba~3.x

Con un update da samba~2.x a samba~3.x non vi sarà più l'autenticazione `winbind`; comunque si potrà continuare a ricorrere agli altri metodi di autenticazione. Per tal motivo sono stati eliminati i seguenti programmi:

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

Si veda anche: `http://www.squid-cache.org/Doc/FAQ/FAQ-23.html#ss23.5`.

Update OpenSSH (versione 3.8p1)

Il supporto `gssapi` è stato sostituito da `gssapi-with-mic` per risolvere degli eventuali attacchi MITM. Le due versioni sono incompatibili, ciò vuol dire che non sarà possibile autenticarvi con ticket Kerberos di distribuzioni precedenti, poiché vengono utilizzati metodi di autenticazione diversi.

Applicazioni SSH e terminal

Durante l'accesso da un host remoto (soprattutto via SSH, telnet e RSH) tra la versione 9 (con UTF-8 nella configurazione standard) e sistemi precedenti (SUSE LINUX 9.0 e precedenti (senza UTF-8 di default o addirittura non supportato), le applicazioni di terminale visualizzeranno i caratteri in maniera non corretta.

Ciò è dovuto al fatto che OpenSSH non inoltra delle impostazioni locali. Quindi le impostazioni di default del sistema possibilmente si discostano da quelle del terminale remoto. Ciò vale per YaST nel modo testo come anche per applicazioni eseguite dall'host remoto dall'utente normale (non da `root`). Ciò vale per applicazioni eseguite da `root` solamente se l'utente modifica i file locale di default validi per `root` (solo `LC_CTYPE` viene impostata di default).

Eliminazione di libiodbc

FreeRADIUS va linkato con unixODBC, dato che non vi è più libiodbc.

Risorse XML in /usr/share/xml

FHS (si veda l'sezione A a pagina 671) prevede che risorse XML (DTD, stylesheet etc.) vengano installate sotto `/usr/share/xml`. Per questo alcune directory non si trovano più sotto `/usr/share/sgml`. In caso di difficoltà si dovrà intervenire sui propri script o makefile oppure utilizzare i cataloghi ufficiali (in particolar modo `/etc/xml/catalog` o `/etc/sgml/catalog`.

Media estraibili e subfs

I media estraibili ora vengono integrati nel sistema tramite subfs. Non è più necessario eseguire `mount` manualmente, è sufficiente entrare nella relativa directory del dispositivo sotto `/media`. Non si potranno espellere dei supporti finquanto un programma vi accede.

4.2.4 Dalla versione 9.1 alla 9.2

Rimandiamo all'articolo "Known Problems and Special Features in SUSE LINUX 9.2" della banca dati di supporto di SUSE sotto `http://portal.suse.com`; parola chiave *special features*.

Abilitare il firewall nella finestra proposte durante l'installazione

SuSEFirewall2, la soluzione firewall fornita a corredo, viene abilitato nella finestra delle proposte alla fine del processo di installazione per incrementare il livello di sicurezza del sistema. Ciò vuol dire che in un primo tempo tutte le porte di sistema sono chiuse e che su richiesta possono essere riaperte nel dialogo delle proposte. Di default non potrete eseguire il log in da sistemi remoti. Ciò interferisce con la navigazione sulla rete ed applicazioni multicast, come SLP, Samba ("Network Neighborhood") ed alcuni giochi. Potete intervenire in modo mirato sulle impostazioni del firewall ricorrendo a YaST.

Se quindi durante il processo di installazione o configurazione di un servizio è richiesto l'accesso di rete, il rispettivo modulo di YaST aprirà tutte le porte TCP e UDP richieste di tutte le interfacce interne e esterne. Se non desiderate che ciò avvenga, potrete chiudere delle porte tramite il modulo YaSTo eseguire altre impostazioni dettagliate che riguardano il firewall.

Tabella 4.2: *Porte richieste dai servizi principali*

Servizio	Porta
Server HTTP	Firewall viene impostato in base alle istruzioni "Listen" (solo TCP)
Mail (postfix)	smtp 25/TCP
Server Samba	netbios-ns 137/TCP; netbios-dgm 138/TCP; netbios-ssn 139/TCP; microsoft-ds 445/TCP
Server DHCP	bootpc 68/TCP
Server DNS	domain 53/TCP; domain 53/UDP
DNS server	in più supporto speciale per portmapper in SuSEFirewall2
Portmapper	sunrpc 111/TCP; sunrpc 111/UDP
NFS server	nfs 2049/TCP
NFS server	in più portmapper

NIS server	abilita portmap
TFTP	tftp 69/TCP
CUPS (IPP)	ipp 631/TCP; ipp 631/UDP

KDE e supporto a IPv6

Di default per KDE il supporto a IPv6 non è abilitato. Potete farlo tramite l'editor `/etc/sysconfig` di YaST. La ragione per la quale questa funzionalità è disabilitata è dovuta al fatto che indirizzi IPv6 non vengono supportati in modo corretto da tutti gli ISP (Internet Service Provider) e che quindi ciò comporterebbe dei messaggi di errore durante la navigazione sul web e dei ritardi in fase di visualizzazione delle pagine web.

YaST Online Update e pacchetti "delta"

Lo YaST Online Update supporta ora dei particolari pacchetti RPM che archiviano solo la differenza binaria di un dato pacchetto base. Ciò permette di ridurre in modo considerevole la dimensione del pacchetto ed il tempo richiesto per il download, ma comporta un più elevato carico di lavoro per la CPU dato che deve riassemblare il pacchetto finale. In `/etc/sysconfig/onlineupdate`, specificate se YOU debba utilizzare i pacchetti "delta." Si veda `file:///usr/share/doc/packages/deltarpm/README` per i dettagli di natura tecnica.

Configurazione del sistema di stampa

Alla fine del processo di installazione (finestra delle proposte) per quanto riguarda la configurazione del firewall si deve assicurare che le porte necessarie al sistema di stampa siano aperte. CUPS richiede che la porta 631/TCP e porta 631/UDP siano aperte per il normale modo operativo. Anche porta 515/TCP (per il vecchio protocollo LPD) e le porte richieste da Samba devono essere aperte se si vorrà stampare tramite LPD o SMB.

Passare a X.Org

Il passaggio da XFree86 a X.Org viene semplificato grazie a dei link di compatibilità che permettono di accedere ai file e comandi di maggior rilevanza anche tramite il loro vecchio nome.

Tabella 4.3: Comandi

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

Tabella 4.4: File di protocollo in /var/log

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

Inoltre, utilizzando X.Org il nome dei pacchetti cambia da `XFree86*` a `xorg-x11*`.

Emulatori di terminale per X11

Abbiamo eliminato una serie di emulatori di terminale per il fatto che non vengono più aggiornati o perché non funzionano nell'ambiente di default, in particolar modo perché non supportano UTF-8. SUSE LINUX offre dei terminali standard come xterm, terminali KDE e GNOME nonché mlterm (Multilingual Terminal Emulator for X) che si propone per la sostituzione di aterm ed eterm.

Modifiche nel pacchetto powersave

I file di configurazione in `/etc/sysconfig/powersave` sono stati modificati:

Tabella 4.5: File di configurazione suddivisi in /etc/sysconfig/powersave

Vecchio	Ora suddiviso in
`/etc/sysconfig/powersave/common`	`common`
	`cpufreq`

```
                                        events
                                        battery
                                        sleep
                                        thermal
```

`/etc/powersave.conf` non esiste più e le variabili sono state spostate nei file riportati nella tabella 4.5 nella pagina precedente. Se avete apportato delle modifiche alle variabili "event" in `/etc/powersave.conf` dovrete eseguire gli adattamenti del caso in `/etc/sysconfig/powersave/events`.

Inoltre, va tenuto presente che è cambiata la terminologia degli stati di "dormiveglia" (ingl. sleep status); in passato vi era:

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

Adesso abbiamo:

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

OpenOffice.org (OOo)

Directory OOo viene ora installato in `/usr/lib/ooo-1.1` al posto di `/opt/OpenOffice.org`. La directory di default per la configurazione dell'utente è ora `~/.ooo-1.1` al posto di `~/OpenOffice.org1.1`.

Wrapper: Vi sono dei nuovi wrapper per l'avvio di componenti OOo; ecco una tabella con i corrispondenti nomi:tabella 4.6 in questa pagina.

Tabella 4.6: *Wrapper*

Vecchio	Nuovo
`/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

Una novità riferita al wrapper è rappresentata inoltre dal supporto alla opzione `--icons-set` per realizzare il passaggio da icone KDE a GNOME e viceversa. Le seguenti opzioni non vengono più supportate: `--default-configuration`, `--gui`, `--java-path`, `--skip-check`, `--lang` (che ora viene rilevata tramite locales), `--messages-in-window` e `--quiet`.

Supporto a KDE e GNOME: Estensioni di KDE e GNOME vengono messe a disposizione nei pacchetti a sé stanti `OpenOffice_org-kde` e `OpenOffice_org-gnome`.

Soundmixer "kmix"

Il soundmixer kmix è preimpostato come standard. Per hardware high-end sono disponibili miscellatori come QAMix/KAMix, envy24control (solo ICE1712) o hdspmixer (solo RME Hammerfall).

Masterizzare DVD

In passato dal pacchetto `cdrecord` veniva applicata una patch al binario `cdrecord`, per supportare la masterizzazione di DVD. Ora invece viene installato il nuovo binario `cdrecord-dvd` che ha questa patch.

L'applicazione `growisofs` dal pacchetto `dvd+rw-tools` consente ora di masterizzare tutti i tipi di DVD (DVD+R, DVD-R, DVD+RW, DVD-RW, DVD+RL). Consigliamo di utilizzare questa applicazione al posto di `cdrecord-dvd` patchato.

Kernel multipli

Sussiste anche la possibilità di installare diversi kernel l'uno accanto all'altro per dare ad esempio agli amministratori di sistema il modo di eseguire un upgrade da un kernel all'altro installando il nuovo kernel e verificare se il nuovo kernel funziona nel modo atteso per poter quindi procedere con la disinstallazione del vecchio kernel. Mentre YaST non supporta ancora questa funzionalità, diversi kernel si lasciano installare e disinstallare in maniera del tutto semplice dalla shell eseguendo `rpm -i` ⟨*`pacchetto`*⟩`.rpm`. Per maggiori dettagli sulla amministrazione di pacchetti dalla linea di comando rimandiamo alla sezione 4.3 a pagina 130.

Il menu del boot loader di default contiene solo una registrazione per il kernel. Prima di installare diversi kernel andrebbe aggiunta una registrazione per ogni ulteriore kernel, per poterli selezionare in modo del tutto semplice. Si può accedere al kernel abilitato prima dell'installazione di uno nuovo tramite `vmlinuz.previous` e `initrd.previous`. Potete accedere al kernel abilitato in precedenza generando una voce del boot loader simile a quella di default e chiamandola `vmlinuz.previous` e `initrd.previous` invece di `vmlinuz` e `initrd`. Un'ulteriore possibilità è data dal fatto che GRUB e LILO supportano registrazioni wild card per il boot loader. Per delle indicazioni dettagliate rimandiamo alle pagine info di GRUB (`info grub`) ed alla pagina di manuale `lilo.conf` (5).

4.2.5 Dalla versione 9.2 alla 9.3

Leggete l'articolo "Known Problems and Special Features in SUSE LINUX 9.3" della banca dati di supporto della SUSE all'indirizzo `http://portal.suse.com`, indicando la come parola chiave *special features*.

Avviare l'installazione manuale al prompt del kernel

Il modo 'Installazione manuale' non viene più visualizzato nella schermata del boot loader. Comunque potete passare nel modo manuale di linuxrc dando `manual=1` al prompt di boot. Di solito ciò non è necessario perché potete impostare le opzioni di installazione direttamente al prompt del kernel, ad es. `textmode=1`, o indicare una URL come origine di installazione.

Autenticazione di rete tramite Kerberos

Al posto di `heimdal` vi è `Kerberos` ad essere preimpostato per l'autenticazione di rete. Non è possibile convertire una configurazione heimdal esistente in modo

automatico. Durante un aggiornamento verranno create delle copie di sicurezza (backup) dei file di configurazione come mostrato nella tabella 4.7 in questa pagina.

Tabella 4.7: *File di backup*

Vecchio file	File di backup
`/etc/krb5.conf`	`/etc/krb5.conf.heimdal`
`/etc/krb5.keytab`	`/etc/krb5.keytab.heimdal`

La configurazione client (`/etc/krb5.conf`) è molto simile a quella di heimdal. Se non è stato impostato qualcosa in modo particolare, basta sostituire il parametro `kpasswd_server` con `admin_server`

Non è possibile assumere i dati relativi al server (kdc/kadmind). Dopo un aggiornamento del sistema la vecchia banca dati di heimdal è ancora disponibile sotto `/var/heimdal`; con MIT kerberos le banca dati la trovate sotto `/var/lib/kerberos/krb5kdc`.

File di configurazione X.Org

Il tool di configurazione SaX2 scrive le impostazioni relative a X.Org in `/etc/X11/xorg.conf`. Se eseguite una installazione ex novo non viene creato un link di compatibilità da `XF86Config` verso `xorg.conf`.

Configurazione PAM

`common-auth` configurazione PAM di default per la sezione auth

`common-account` configurazione PAM di default per la sezione account

`common-password` configurazione PAM di default per la modifica password

`common-session` configurazione PAM di default per l'amministrazione della sessione

Si consiglia di includere le configurazioni di default dai file di configurazione relativi alla vostra applicazione, perché è più facile tenere aggiornato e modificare un solo file di configurazione invece che ca. 40 file (che vi erano sul sistema). Se

installate una applicazione in un secondo momento, essa erediterà le modifiche apportate e l'amministratore non dovrà adattare la configurazione.

Le modifiche sono semplici: se avete il seguente file di configurazione (dovrebbe essere il default per la maggioranza delle applicazioni):

```
#%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
```

basta apportare queste modifiche:

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

4.3 RPM— il package manager

SUSE LINUX ricorre a RPM (Red Hat Package Manager) che come programmi principali per l'amministrazione dei pacchetti software dispone di `rpm` e `rpmbuild`. In tal modo gli utenti, gli amministratori di sistema e anche coloro che assemblano dei pacchetti dispongono di un potente database, e così di informazioni dettagliate in qualsiasi momento, sul software installato.

Essenzialmente `rpm` può agire in cinque modi: installare/disinstallare o aggiornare dei pacchetti software, ricreare la banca dati RPM, inviare richieste alla banca dati RPM o a singoli archivi RPM, controllare l'integrità dei pacchetti e firmare pacchetti. `rpmbuild` crea pacchetti da poter installare da sorgenti cosiddette pristine, cioé non modificati.

Gli archivi RPM installabili vengono compressi in uno speciale formato binario; gli archivi sono composti da file da installare e da diverse meta-informazioni che vengono usate da `rpm` durante l'installazione stessa per configurare il relativo pacchetto software, o che vengono archiviate nel database RPM a scopo documentativo. Gli archivi RPM hanno l'estensione `.rpm`.

Con `rpm` potete amministrare pacchetti conformi allo standard LSB; su LSB cfr. la sezione A a pagina 671.

Suggerimento

Nel caso di alcuni pacchetti, le componenti necessarie allo sviluppo di software (biblioteche, file header ed include, ecc.) sono state raccolte in pacchetti a se stanti. Questi pacchetti sono necessari soltanto quando si intende compilare *da soli* del software (ad esempio, nuovi pacchetti GNOME). Generalmente, questi pacchetti sono riconoscibili dall'estensione `-devel`: `alsa-devel`, `gimp-devel` e `kdelibs-devel`.

Suggerimento

4.3.1 Controllare l'autenticità di un pacchetto

I pacchetti RPM di SUSE LINUX vengono firmati con GnuPG; ecco la chiave compreso il fingerprint:

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

Con il comando `rpm --checksig apache-1.3.12.rpm` potete controllare la firma di un pacchetto RPM e in questo modo stabilire se proviene veramente da SUSE o da una altra fonte affidabile. Cosa consigliabile specialmente quando si scaricano pacchetti di aggiornamento da Internet. Di default, la nostra chiave pubblica per firmare i pacchetti si trova in `/root/.gnupg/`. A partire dalla versione 8.1, la chiave si trova inoltre nella directory `/usr/lib/rpm/gnupg/`, in modo da consentire anche all'utente normale di controllare la firma dei pacchetti RPM.

4.3.2 Amministrare i pacchetti: installarli, aggiornarli e disinstallarli

Normalmente, installare un archivio RPM é una questione di pochi attimi: `rpm -i` ⟨*`pacchetto`*⟩`.rpm`. Con questo comando, un pacchetto viene installato solo se sono rispettate le dipendenze e se non vi sono dei conflitti. Tramite una comunicazione d'errore, `rpm` richiede i pacchetti necessari all'adempimento delle dipendenze. In background, il database fa la guardia che non vi siano dei conflitti: di norma un file può appartenere solo ad un pacchetto. Con diverse opzioni, é possibile aggirare questa regola; chi lo fa deve sapere perfettamente ciò che

sta facendo, poiché si può compromettere la capacità del sistema di eseguire un aggiornamento.

Di sicuro interesse sono anche le opzioni `-U` o `--upgrade` e `-F` o `--freshen` per aggiornare un pacchetto. `rpm -F` ⟨*`pacchetto`*⟩`.rpm`. Questo comando cancella la versione vecchia del pacchetto e installa quella nuova. La differenza tra le due opzioni é che con `-U` vengono installati anche pacchetti che finora non erano disponibili nel sistema, mentre con l'opzione `-F` un pacchetto viene aggiornato solo se era già installato in precedenza. Contemporaneamente `rpm` cerca di intervenire con circospezione sui file di configurazione applicando la seguente strategia:

- Se un file di configurazione non é stato modificato dall'amministratore di sistema, `rpm` installa la nuova versione del file in questione. Un intervento da parte dell'amministratore non é più necessario.
- Se un file di configurazione é stato modificato prima dell'aggiornamento, `rpm` memorizzerà con l'estensione `.rpmorig` o `.rpmsave` (file di backup) il file modificato e installerà la nuova versione del pacchetto RPM solo nel caso vi siano delle differenze tra il file originale e il file del pacchetto aggiornato. In questo caso é molto probabile che dobbiate adattare il file di configurazione appena installato in base alla copia di sicurezza (`.rpmorig` o `.rpmsave`). In seguito, assicuratevi di aver eliminato tutti i file `.rpmorig` e `.rpmsave` per evitare l'insorgere di difficoltà durante futuri aggiornamenti.
- I file `.rpmnew` appaiono se il file di configurazione esiste già *e* se nel file `.spec` é stato attivato `noreplace`.

Alla fine di un update, dopo l'adattamento, si devono rimuovere tutti i file `.rpmsave` e `.rpmnew` per non essere d'impaccio ai futuri aggiornamenti. L'estensione `.rpmorig` si ha se il file non è stato riconosciuto dalla banca dati RPM.

Altrimenti si ha l'estensione `.rpmsave`. Cioé: `.rpmorig` si ha quando si esegue l'update da un formato estraneo ad RPM; `.rpmsave` si ha all'update dall'RPM vecchio all'RPM nuovo. Con `.rpmnew` non si può dire se l'amministratore abbia modificato il file di configurazione o meno. Un elenco di questi file lo trovate sotto `/var/adm/rpmconfigcheck`. Tenete presente che alcuni file di configurazione (p.es. `/etc/httpd/httpd.conf`) non vengono sovrascritti di proposito, affinché vi sia continuità di funzionamento.

L'opzione `-U` é dunque più che un equivalente della sequenza `-e` (disinstallare/cancellare) ed `-i` (installare). Ogni qualvolta sia possibile é consigliabile usare l'opzione `-U`.

`rpm-e` ⟨*pacchetto*⟩. `rpm` elimina un pacchetto solo quando non esistono più delle dipendenze;. p.es. é impossibile cancellare Tcl/Tk finché sia richiesto da un programma; anche qui fa la guardia RPM con il suo database. Se, in casi eccezionali, non é possibile cancellare un pacchetto, benché non ci sia alcuna dipendenza, può essere d'aiuto ricostruire il database RPM con l'aiuto dell'opzione `--rebuilddb`.

4.3.3 RPM e patch

Per garantire la sicurezza di un sistema é necessario di tanto in tanto installare dei pacchetti che lo aggiornano. Finora un bug in un pacchetto si lasciava eliminare solo se si sostituiva l'intero pacchetto. Nel caso di grossi pacchetti con piccoli errori si raggiungeva subito una considerevole quantità di dati. SUSE offre adesso una nuova funzionalità RPM che consente di installare delle patch per pacchetti.

Prendiamo pine come esempio:

La RPM patch è adatta per il mio sistema?
Per verificare ciò, stabilite la versione installata del pacchetto. Nel caso di pine il comando è:

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

Quindi bisogna verificare se la RPM patch va bene per la versione in questione di pine con:

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

Questa patch va bene per tre diverse versioni di pine. Viene elencata anche la versione installata nell'esempio, quindi la patch può essere installata.

Quali file saranno sostituiti dalla patch?
La RPM patch indica i file interessati. Il parametro `rpm -P` consente di selezionare particolari feature delle patch. Per avere l'elenco dei file servitevi del seguente comando:

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

oppure, se la patch è già installata, eseguite il seguente comando:

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

Come installare una RPM patch nel sistema?
Le RPM patch non si distinguono più di tanto dai consueti RPM. L'unica differenza è che deve essere già installato un RPM adatto.

Quali patch sono già installate e per quale versione del pacchetto?
Con `rpm -qPa` visualizzate tutte le patch installate. Se nel sistema è stata installata solo una patch (come nel nostro esempio), l'elenco avrà il seguente aspetto:

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

Se in un secondo momento volete sapere quale versione di un pacchetto era installata originariamente, eseguite (nel caso di `pine`) questo comando:

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

Ulteriori informazioni, anche sulle funzionalità della RPM patch, sono reperibili nella pagina di manuale di `rpm` e `rpmbuild`.

4.3.4 Pacchetti RPM delta

I pacchetti "delta RPM" contengono la differenza (appunto il "delta") tra la vecchia e nuova versione di un pacchetto RPM. Applicando un delta RPM su un vecchio RPM si generà un RPM completamento nuovo, senza che abbiate bisogno di una copia del vecchio RPM, visto che un delta RPM è applicabile anche su un RPM installato. I pacchetti deltarpm sono più piccoli di una RPM patch, cosa che si rivela essere un vantaggio quando si tratta di trasmettere dei

pacchetti di aggiornamento tramite Internet. Lo svantaggio è che in fase di aggiornamento con RPM delta si genera un maggior numero di cicli CPU rispetto a RPM comuni o patch. Per fare in modo che YaST utilizzi dei pacchetti RPM delta durante delle sessioni YOU, impostate `YOU_USE_DELTAS` su "yes" in `/etc/sysconfig/onlineupdate`.

I binari `prepdeltarpm`, `writedeltarpm` e `applydeltarpm` sono parte della deltarpm suite e vi permettono di creare e applicare pacchetti delta RPM. Con il seguente comando create un RPM delta denominato `new.delta.rpm` (se vi sono un `old.rpm` e `new.rpm`:

```
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
```

Con `applydeltarpm` potete ricostruire il nuovo RPM anche dal file system se il vecchio pacchetto è già installato:

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

O utilizzate l'opzione `-r` se volete derivare il nuovo RPM da quello vecchio senza accedere al file system:

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

Si veda `file:///usr/share/doc/packages/deltarpm/README` for technical details.

4.3.5 Inviare richieste

Con l'opzione `-q` (ingl.query) si crea una richiesta che permette di rovistare nell' archivio RPM (aggiungendo l'opzione `-p`) e interrogare la banca dati RPM dei pacchetti installati. Specificando dei parametri si otterranno in modo mirato le informazioni richieste; si veda la tabella 4.8 nella pagina successiva.

Tabella 4.8: *Le opzioni per l'invio di richieste di maggior importanza*

`-i`	Informazioni sul pacchetto
`-l`	Elenco file
`-f FILE`	Interroga il pacchetto contenente il file ⟨*FILE*⟩ (va specificato il percorso completo di ⟨*FILE*⟩)
`-s`	Elenco file con informazioni sullo stato (implica `-l`)
`-d`	Elenca solo file di documentazione (implica `-l`)
`-c`	Elenca solo file di configurazione (implica `-l`)
`--dump`	Elenco file dettagliato (da utilizzare con `-l`, `-c` oppure `-d`)
`--provides`	Elenca le funzionalità del pacchetto che un altro pacchetto può richiedere tramite `--requires`
`--requires`, `-R`	Quanto il pacchetto richiede
`--scripts`	Script di installazione (preinstall, postinstall, uninstall)

Ad esempio, il comando `rpm -q -i wget` visualizza le informazioni mostrate nell'esempio 4.2 in questa pagina.

Esempio 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 can be done in script files or via the command line.
[...]
```

L'opzione `-f` produce l'effetto desiderato se si specifica il nome del file completo, incluso il percorso; si può inserire una quantità qualsiasi di nomi di file, p.es.:

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

produce come risultato:

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

Se conoscete solo una parte del nome del file, utilizzate uno shell script (cfr. l'esempio 4.3 in questa pagina); il nome del file cercato é da indicare come parametro alla chiamata dello script.

Esempio 4.3: *Script cerca-pacchetti*

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

Con il comando `rpm -q --changelog rpm` vi fate mostrare l'elenco informazioni (update, configurazione, modifiche etc.) su un determinato pacchetto; si veda nell'esempio il pacchetto `rpm`: Tuttavia, vengono visualizzate solo le ultime 5 voci della banca dati RPM: nel pacchetto sono però contenute tutte le voci (degli ultimi due anni): se il CD 1 é montato su `/media/cdrom` potete fare la vostra richiesta.

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

In base alla banca dati RPM installata, si possono anche eseguire dei controlli; queste operazioni vengono avviate con l'opzione `-V` (equivale a `-y` o `--verify`). Con questa opzione si induce `rpm` a mostrare tutti quei file che sono stati modificati rispetto alla versione attualmente installata. `rpm` antepone al nome di file vero e proprio fino ad otto caratteri, i quali indicano le seguenti modifiche:

Tabella 4.9: *RPM: opzioni di controllo*

`5`	Somma di controllo MD5
`S`	Dimensione file
`L`	Link simbolico
`T`	Ora della modifica
`D`	Num. di dispositivo maggiore e minore
`U`	Proprietario
`G`	Gruppo
`M`	Modo (permessi e tipo di file)

Nei file di configurazione viene emessa anche una `c`. Per esempio, nel caso sia stata apportata qualche modifica a `/etc/wgetrc` di `wget`:

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

I file della banca dati RPM si trovano sotto `/var/lib/rpm`. Con una partizione `/usr` di 1 Gbyte, la banca dati può riservarsi quasi 30 Mbyte di spazio sull' hard disk; specialmente dopo un aggiornamento completo. Se la banca dati sembra essere troppo grande é sempre d'aiuto crearne (con l'opzione `--rebuilddb`) una nuova sulla base di quella già esistente; non nuoce mai fare una copia di sicurezza prima di eseguire un rebuild. Lo script `cron` `cron.daily` deposita le copie giornaliere compresse della banca dati sotto `/var/adm/backup/rpmdb`, la cui quantità viene determinata dalla variabile `MAX_RPMDB_BACKUPS` (standard: `5`) in `/etc/sysconfig/backup`; si deve contare con fino a 3 Mbyte per ogni back-up con una `/usr` di 1 Gbyte.

4.3.6 Installare e compilare i sorgenti

Tutti i sorgenti di SUSE LINUX terminano in `.src.rpm`, ossia RPM sorgenti.

Suggerimento

Come tutti i pacchetti, anche questo tipo di pacchetti può venir installato tramite YaST i sorgenti non vengono però mai contrassegnati come installati (`[i]`), come è invece il caso per pacchetti normali. Ciò dipende dal fatto che i sorgenti non vengono registrati nella banca dati RPM; quando installate un sorgente, si aggiunge solo il codice sorgente al sistema. Il software in sé deve essere compilato. La banca dati RPM infatti indica solo software *installato*.

Suggerimento

Le seguenti directory devono essere disponibili per `rpm` e `rpmbuild` sotto `/usr/src/packages` (nel caso non si siano fatte delle impostazioni proprie p.es. in `/etc/rpmrc`):

`SOURCES` per i sorgenti originali (file `.tar.bz2` o `.tar.gz` etc.) e per gli adattamenti specifici della distribuzione (di solito `.diff` o `.patch`).

`SPECS` per i file `.spec` che alla stregua dei meta-makefile controllano il processo*build*.

`BUILD` sotto questa directory si scompattano, si adattano (ingl. patched) e si compilano i sorgenti.

`RPMS` qui vengono archiviati i pacchetti binari pronti.

`SRPMS` e qui i *source* RPM.

Se installate un pacchetto sorgente con YaST, le componenti necessarie per il processo build, vengono installate sotto `/usr/src/packages`: i sorgenti e gli adattamenti sotto `SOURCES` ed i rispettivi file `.spec` sotto `SPECS`.

Avvertimento

Non fate degli esperimenti con componenti importanti del sistema (`glibc`, `rpm`, `sysvinit`, etc.); altrimenti mettete a repentaglio la funzionalità del vostro sistema.

Avvertimento

Osserviamo ora da vicino il pacchetto `wget.src.rpm`. Dopo aver installato il pacchetto con YaST si avrà più o meno questo elenco:

```
/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 `rpmbuild -b`$\langle X \rangle$ `/usr/src/packages/SPECS/wget.spec` viene inizializzato il processo di compilazione; la variabile $\langle X \rangle$ può indicare diversi stadi del processo build (cfr. l'output di `--help` o la documentazione RPM); segue una breve descrizione:

`-bp` preparare i sorgenti nella directory `/usr/src/packages/BUILD`: decomprimere e adattare (ingl.patch).

`-bc` come `-bp` con compilazione.

`-bi` come `-bc` con installazione; ATTENZIONE, se il pacchetto non supporta la feature BuildRoot, può accadere che durante l'installazione vengano sovrascritti importanti file di configurazione!

`-bb` come `-bi`, con creazione del pacchetto binario; se tutto é andato per il verso giusto, lo ritrovate in `/usr/src/packages/RPMS`.

`-ba` come `-bb`, con creazione del cosiddetto RPM sorgente; se tutto é andato per il verso giusto, si trova in `/usr/src/packages/SRPMS`.

`--short-circuit` con questa opzione potete saltare i singoli passi.

L'RPM binario creato può venir installato adesso con `rpm-i` o meglio con `rpm-U`. Se eseguite l'installazione con `rpm`, il pacchetto comparirà nella banca dati RPM.

4.3.7 Compilare pacchetti RPM con build

Nel caso di molti pacchetti sussiste il pericolo che durante la loro compilazione si aggiungono involontariamente dei file al sistema in esecuzione. Per evitare che questo avvenga potete usare `build` che crea un ambiente ben definito in cui assemblare il pacchetto. Per creare un ambiente chroot, lo script di `build` deve disporre di un albero di pacchetti completo che può trovarsi sul disco rigido o essere

messo a disposizione tramite NFS o trovarsi anche su un DVD. Basta comunicarlo allo script con il comando `build --rpms ⟨directory⟩`. A differenza di `rpm`, il comando `build` cerca il file SPEC nella stessa directory dei sorgenti. Se come nell'esempio riportato sopra volete ricompilare wget e il DVD é montato sotto `/media/dvd`, immettete i seguenti comandi come `root`:

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

Sotto `/var/tmp/build-root` viene creato un ambiente minimale in cui assemblare il pacchetto. In seguito i pacchetti creati si trovano sotto `/var/tmp/build-root/usr/src/packages/RPMS`

Lo script `build` mette ancora un serie di altre opzioni a vostra disposizione. Potrete utilizzare propri RPM, non inizializzare l'ambiente build o limitare il comando `rpm` ad uno degli stadi descritti sopra. Per avere maggiori dettagli digitate il comando `build --help` e consultate la pagina di manuale di `build`.

4.3.8 Tool per archivi RPM e la banca dati RPM

Midnight Commander (`mc`) é, di per sé, in grado di mostrare il contenuto di un archivio RPM e di copiarne delle parti. Midnight Commander raffigura gli archivi come file system virtuali, in tal modo sono disponibili le solite voci di menu di Midnight Commander: le informazioni `HEADER` possono venire visualizzate premendo (F3); con i tasti-cursore e con (Invio) é possibile navigare nell'archivio, e all'occorrenza copiarne delle componenti con (F5).

KDE contiene il tool kpackage quale front-end per `rpm`. Un gestore dei pacchetti davvero completo è disponibile sotto forma di modulo YaST (si veda la sezione 2.2.1 a pagina 40).

Riparazione del sistema

YaST offre oltre ad una serie di moduli per l'installazione e la configurazione del sistema anche delle funzionalità per riparare il sistema installato. Questo capitolo descrive una serie di modi per rimettere a sesto il sistema. Il sistema di salvataggio SUSE permette di accedere alle partizioni, cosa che permetterà ad un amministratore di sistema esperto di riparare un sistema danneggiato.

Dato che un sistema danneggiato non esegue correttamente il boot, e un sistema in esecuzione si lascia riparare con difficoltà, avviate il sistema come se doveste eseguire una nuova installazione. Seguite le indicazione contenute nel capitolo 1 a pagina 3 per arrivare al dialogo di selezione del tipo di installazione: scegliete l'opzione 'Riparazione del sistema installato'.

Importante

Selezione del mezzo di installazione

Per la riparazione di un sistema installato utilizzate solo i mezzi di installazione corrispondenti.

Importante

In seguito selezionate il modo in cui eseguire la riparazione del sistema: riparazione automatica, personalizzata o tramite dei tool per esperti. Tutte le opzioni disponibili verranno illustrate in questo capitolo.

5.1 Riparazione automatica

Il metodo migliore di ripristinare un sistema danneggiato, se non si sa bene quale e dove sia il danno. Il programma, prima di tutto, analizza minutamente il sistema. Questa procedura richiede del tempo e la sua progressione viene visualizzata in basso tramite due barre di progressione. La barra superiore mostra il progresso della verifica attuale, mentre la barra inferiore mostra l'andamento dell'analisi complessiva. Al di sopra delle barre, viene visualizzato il protocollo dell'analisi, con descrizione e risultato delle singole verifiche (Si veda la figura 5.1 a fronte). Vengono eseguiti i seguenti test. Ogni test, a sua volta, comprende una miriade di singole verifiche.

Tabella delle partizioni dei dischi rigidi rilevati
: Il programma verifica la validità e la coerenza delle tabelle di partizionamento di tutti i dischi rigidi rilevati.

Partizioni swap Il programma cerca e testa i settori swap del sistema installato. Vi potrebbe anche venir chiesto se debba esserne attivato uno: confermate dato che l'attivazione di una partizione swap accelera il processo di riparazione.

File system Il programma analizza singolarmente tutti i file system rilevati

Registrazioni del file `/etc/fstab` Il programma verifica che tutte le registrazioni di questo file siano complete e coerenti e, in seguito, monta tutte le partizioni valide.

Configurazione del bootloader Il programma verifica la completezza e coerenza della configurazione del bootloader del sistema (GRUB o LILO), esaminando il dispositivi di boot e root nonché la disponibilità dei moduli initrd.

Banca dati dei pacchetti Il programma verifica che la banca dati contenga tutti i pacchetti necessari all'installazione minima. Potete anche far analizzare i pacchetti di base, ma tenete presente che, trattandosi di un numero davvero elevato, questo tipo di esame durerà un bel pò.

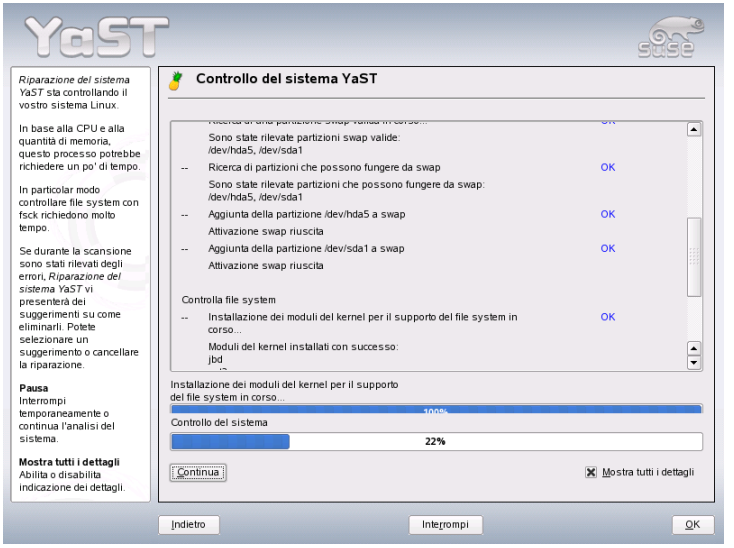

Figura 5.1: *Il modo di riparazione automatica*

Ogni volta che viene rilevato un errore, il programma interrompe l'analisi ed apre una finestra che descrive il problema e le possibili soluzioni. Qui, la casistica è infinita, ragion per cui non entreremo nel dettaglio in questa sede. Vi preghiamo, tuttavia, di leggere attentamente il contenuto della finestra, prima di fare la vos-

tra scelta. In caso di dubbio, potete sempre rifiutare la riparazione. In questo caso, il sistema rimane inalterato: il programma non prende mai automaticamente l'iniziativa quando si tratta di riparazione del sistema.

5.2 Riparazione personalizzata

La riparazione automatica esegue categoricamente tutte le verifiche e test. Pertanto, si consiglia di ricorrervi solo quando non si sa dove e quale sia il danno. Se, invece, sapete già quale parte del sistema è danneggiata, potete ridurre il numero di verifiche del programma: nel dialogo iniziale, scegliete 'Riparazione personalizzata' e vi verrà mostrata una lista di gruppi di test, con tutte le caselle contrassegnate da una crocetta. Se la lasciate così, quindi, la riparazione personalizzata avrà l'identica portata di quella automatica. Se siete sicuri che determinati settori del sistema *non* siano danneggiati, escludeteli dalla verifica, deselezionando la casella. Dopodiché, cliccate su 'Avanti' e verrà avviata un'analisi (a seconda dei casi, anche notevolmente) più breve di quella automatica.

Attenzione: non tutti i gruppi possono essere deselezionati singolarmente: ad esempio, la verifica del contenuto di fstab viene sempre fatta insieme a quella dei file system e delle partizioni swap. Se necessario, sarà YaST ad assicurare il rispetto di queste dipendenze, selezionando automaticamente il minor numero di verifiche strettamente necessarie all'esecuzione di un determinato test.

5.3 Tool per esperti

Gli esperti di SUSE LINUX che sanno già dove porre mano, possono scegliere anche l'opzione 'Riparazione da esperti'.

Installare un nuovo bootloader Questa opzione corrisponde ad un modulo di YaST per la configurazione del bootloader. Per maggiori dettagli, vi preghiamo di consultare la sezione 8.4 a pagina 190.

Avviare il partizionatore Con questa opzione, si avvia il partizionatore di YaST per esperti. Per maggiori dettagli, vi preghiamo di consultare la sezione 2.7.5 a pagina 73.

Riparazione del file system Per testare i file system del sistema. Il programma vi mostra, per prima cosa, un elenco di tutte le partizioni rilevate. Poi, scegliete voi quella da sottoporre alla verifica.

Ripristinare partizioni perse Quando una delle vostre tabelle delle partizioni è danneggiata, potete ricorrere a questo modulo per ripararla. Se avete più di un disco rigido, il programma vi presenta un elenco di quelli rilevati. Cliccando 'OK' si avvia la verifica. La durata dipende dalla dimensione della partizione e dalle risorse del vostro sistema.

Importante

Ripristinare la tabella delle partizioni

Questo è un processo delicato. YaST analizza il settore dati del del disco rigido e tenda di rilevare la partizione andata persa. Se ci riesce, i dati verranno reinseriti nella tabella delle partizioni ripristinata. Questo processo comunque non sempre riesce a produrre il risultato desiderato.

Importante

Salvare impostazioni del sistema su dischetto
Questa opzione vi permette di memorizzare i file di sistema più importanti su un dischetto, di modo che, in caso di danni, potete ripristinarli dal dischetto.

Verificare il software installato Questa opzione verifica la coerenza della banca dati dei pacchetti e la disponibilità dei pacchetti più importanti. Se uno dei pacchetti è danneggiato, potete usare questo modulo per reinstallarlo.

5.4 Il sistema di salvataggio di SUSE

SUSE LINUX contiene un sistema di salvataggio che permette in caso di necessità di accedere dall'esterno alle vostre partizioni Linux. Potete caricare il *Sistema di salvataggio* dal CD, via rete o dal server FTP di SUSE. Sono diverse le utility che compongono il sistema di salvataggio con il quale potrete risolvere dei problemi dovuti ad hard disk inaccessibili, file di configurazione corrotti etc.

Parted (`parted`) è una componente del sistema di salvataggio che vi permette di modificare le dimensioni delle partizioni. In caso di necessità potete lanciare questo programma dal sistema di salvataggio se non volete ricorrere al resizer integrato in YaST. Delle informazioni su Parted sono reperibili all'indirizzo: `http://www.gnu.org/software/parted/`

5.4.1 Lanciare il sistema di salvataggio

Avviate il vostro sistema come per l'installazione. Selezionate la voce sistema di salvataggio. Il sistema di salvataggio a questo punto viene decompresso, caricato in una ramdisk come file system root, montato e inizializzato.

5.4.2 Lavorare con il sistema di salvataggio

Se premete (Alt)-(F1) fino a (Alt)-(F3), il sistema di salvataggio vi mette a disposizione almeno tre console virtuali tramite le quali potrete eseguire il login come utente `root` senza la password. Con (Alt)-(F10) entrate nella console del sistema che contiene le comunicazioni del kernel e di syslog.

Sotto `/bin` trovate la shell detta anche finestra di comando e utility (p.es. mount). Importanti utility per file e la rete per controllare e riparare il file system (reiserfs, e2fsck) si trovano sotto `/sbin`. In `/sbin` trovate anche i file binari più importanti per l'amministrazione del sistema come fdisk, mkfs, mkswap, mount, init e shutdown, e per l'amministrazione della rete, come ifconfig, route e netstat. La directory `/usr/bin` contiene l'editor vi, grep, find, less e telnet.

Accesso al sistema normale

Per montare il vostro sistema SUSE LINUX sul disco rigido, vi è il punto di mount `/mnt`; naturalmente, siete liberi di creare anche un'altra directory e usarla come punto di mount. Nel seguente esempio illustriamo la procedura per un sistema con i dettagli di `/etc/fstab` riportato nell'esempio 5.1 in questa pagina.

Esempio 5.1: *Esempio /etc/fstab*

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

Avvertimento

Nella seguente sezione fate attenzione alla sequenza in cui i singoli dispositivi devono venire montati.

Avvertimento

Per avere accesso al vostro sistema, eseguite il mount passo per passo sotto `/mnt` con seguenti comandi:

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

Ora avete accesso a tutto il vostro sistema e potete per esempio correggere degli errori nei file di configurazione come ad es. `/etc/fstab`, `/etc/passwd`, `/etc/inittab` che si trovano ora sotto `/mnt/etc` invece che sotto `/etc`. Perfino partizioni che erano andate completamente perse si possono recuperare con fdisk; si consiglia vivamente di stampare su carta quanto contenuto in `/etc/fstab` nonché l'output del comando `fdisk -l`.

Riparare i file system

File system danneggiati richiedono l'utilizzo del sistema di salvataggio. Di solito i file system non si lasciano riparare con il sistema in esecuzione. In caso di serie difficoltà a volte non sarà neanche possibile eseguire il mount del vostro file system root e l'avvio del sistema sfocia in un `kernel panic`. L'unica cosa da fare in questi casi è quella di provare ad eseguire la riparazione dall'esterno con un sistema di salvataggio.

Nel sistema di salvataggio di SUSE LINUX sono contenute le utility reiserfsck, e2fsck e, per la diagnosi, dumpe2fs. Con esse avrete la meglio sulla maggior parte dei problemi. Poiché, in caso di emergenza, non avrete più accesso neanche alla pagina di manuale di reiserfsck o e2fsck, le trovate annesse nell'sezione B a pagina 673 e nell'sezione B a pagina 677.

Se non è possibile eseguire il mount di un file system `ext2`, a causa di un *Superblocco non valido* in un primo momento fallirà anche `e2fsck`. In tal caso anche il superblocco potrebbe essere corrotto. La soluzione consiste nell'usare una delle copie del superblocco disponibili ogni 8192 blocchi (8193, 16385...). Se il vostro superblocco è corrotto, provate con una delle sue copie, servendovi ad esempio del comando `e2fsck -f -b 8193 /dev/partizionedanneggiata`. L'opzione `-f` forza la verifica del file system e previene in questo modo il possibile errore di e2fsck, il quale, trovando la copia intatta del superblocco, pensa che sia tutto a posto.

Parte II

Sistema

Applicazioni a 32 bit e a 64 bit in un ambiente a 64 bit

SUSE LINUX è disponibile per diverse piattaforme a 64 bit. Questo non significa necessariamente che tutte le applicazioni contenute siano già state portate al modo a 64 bit. SUSE LINUX supporta l'utilizzo di applicazioni a 32 bit in un ambiente a 64 bit. Il presente capitolo vi offre una breve rassegna del modo in cui viene implementato il supporto di applicazioni a 64 bit su piattaforme SUSE LINUX. Viene anche spiegato come vengono eseguite le applicazioni a 32 bit (supporto runtime) e come dovrebbero essere compilate le applicazioni affinché possano essere eseguite sia in ambienti a 32 bit sia in ambienti a 64 bit. Sono inoltre presenti informazioni sulle API del kernel e una spiegazione di come le applicazioni a 32 bit possono essere eseguite in un kernel a 64 bit.

Per le piattaforme a 64 bit AMD64 ed EM64T SUSE LINUX è stato implementato in modo che applicazioni a 32 bit già presenti siano eseguibili "out-of-the-box" in un ambiente a 64 bit. Grazie a questo supporto sussiste la possibilità di continuare a utilizzare le vostre applicazioni a 32 bit preferite senza dover attendere che sia messo a disposizione un rispettivo port al modo a 64 bit.

6.1 Supporto runtime

Importante

Conflitto tra la versione a 32 bit e 64 bit di una applicazione

Se una applicazione è disponibile sia nel modo a 32 bit che a 64 bit, l'installazione parallela di entrambe le versioni comporterà inevitabilmente delle difficoltà. In questi casi dovrete stabilire quale delle due versioni disponibili installare e utilizzare.

Importante

Ogni applicazione richiede una serie di librerie per poter essere eseguita correttamente. Purtroppo le denominazioni delle librerie per versioni a 32 bit e 64 bit sono identiche, va quindi trovato un modo diverso per distinguere l'una dall'altra.

Per mantenere la compatibilità con la versione a 32 bit, le librerie vengono archiviate esattamente proprio là dove lo sono anche in un ambiente a 32 bit. La versione a 32 bit di `libc.so.6` si trova sia in un ambiente a 32 bit che in uno a 64 bit sotto `/lib/libc.so.6`.

Tutte le librerie a 64 bit e i file oggetto vengono archiviati in directory denominate `lib64`, ciò significa che i file oggetto a 64 bit che normalmente andreste a cercare sotto `/lib`, `/usr/lib` e `/usr/X11R6/lib` adesso si trovano sotto `/lib64`, `/usr/lib64` e `/usr/X11R6/lib64`. Di conseguenza le librerie a 32 bit sono reperibili sotto `/lib`, `/usr/lib` e `/usr/X11R6/lib` mentre il nome file per entrambi le versioni può essere mantenuto invariato.

In linea di massima le sottodirectory delle directory contenenti i file oggetto, il cui contenuto non dipende dalla dimensione della parola (ingl. word size) *non* sono state spostate. Ad esempio i font di X11 saranno come di consueto sotto `/usr/X11R6/lib/X11/fonts`.

Questo schema è conforme all'LSB (Linux Standards Base) e al FHS (File System Hierarchy Standard).

6.2 Sviluppo software

Con una toolchain di sviluppo bi-piattaforma è possibile generare oggetti sia a 32 bit che a 64 bit. Di default si ha la compilazione di oggetti a 64 bit. Utilizzando flag speciali si potranno generare oggetti a 32 bit. Per GCC si ha il flag `-m32`.

Tenete presente che tutti i file header vanno scritti in una forma congrua alla piattaforma e che le librerie a 32 bit ed a 64 bit installate debbano avere un'API (Application Programming Interface) adatta ai file header installati. L'ambiente SUSE standard è stato concepito secondo questo schema; se utilizzate delle librerie che avete modificato, dovete provvedere voi.

6.3 Compilare del software su architetture bi-piattaforma

Per sviluppare dei binari su una architettura bi-piattaforma destinati rispettivamente all'altra architettura vanno installate anche le corrispondenti librerie della seconda piattaforma. Questi pacchetti si chiamano `rpmname-32bit`. Inoltre sono richiesti i rispettivi header e librerie che trovate nei pacchetti `rpmname-devel` come anche le librerie di sviluppo per la seconda architettura che troverete sotto `rpmname-devel-32bit`.

La maggior parte dei programmi a sorgente aperto utilizza una configurazione di programma basato su `autoconf`. Per utilizzare `autoconf` ai fini della configurazione di un programma per la seconda architettura si devono sovrascrivere le impostazioni standard del compiler e linker di `autoconf` tramite l'invocazione dello script `configure` con variabili di ambiente aggiuntive.

Il seguente esempio si riferisce a un sistema AMD64 e EM64T con x86 quale seconda piattaforma:

- Impostate `autoconf` in modo che utilizzi il compiler a 32 bit:

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

- Impostate il linker per elaborare oggetti a 32 bit:

  ```
  LD="ld -m elf_i386"
  ```

- Impostate l'assembler per generare oggetti a 32 bit:

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

- Stabilite che le librerie per `libtool` provengono da `/usr/lib64`:

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

- Stabilite che le librerie siano archiviate nella sottodirectory `lib`:

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

- Stabilite l'uso di librerie X a 32 bit:

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

I singoli programmi non richiedono tutte le variabili riportate. Regolatevi a seconda del programma in questione.

6.4 Particolarità del Kernel

I kernel a 64 bit per AMD64 ed EM64t offrono una kernel-ABI (Application Binary Interface) sia nel modo a 64 bit che a 32 bit. Quest'ultima è identica all'ABI del corrispondente kernel a 32 bit, il che significa che applicazioni a 32 bit possono comunicare con un kernel a 64 bit nella maniera in cui lo fanno con un kernel a 32 bit.

Tenete presente che l'emulazione a 32 bit delle chiamate di sistema di un kernel a 64 bit non supporta tutta una serie di API a cui ricorrono dei programmi di sistema. Questo può variare da piattaforma a piattaforma. Per tal ragione un certo numero di applicazioni, tra cui `lspci` oppure programmi di amministrazione LVM devono esistere sotto forma di programmi a 64 bit per garantire un funzionamento corretto.

Un kernel a 64 bit carica esclusivamente moduli di kernel a 64 bit compilati appositamente per il kernel in questione. Non è possibile utilizzare moduli di kernel a 32 bit.

Suggerimento

Alcune applicazioni richiedono propri moduli caricabili dal kernel. Se avete intenzione di utilizzare una applicazione a 32 bit del genere in un ambiente di sistema a 64 bit, rivolgetevi al fornitore dell'applicazione e a SUSE per essere sicuri che la versione a 64 bit del modulo caricabile dal kernel e la versione a 32 bit del kernel API per il modulo in questione siano disponibili.

Suggerimento

L'avvio e la configurazione di un sistema Linux

L'avvio di sistema Linux è un processo di una certa complessità. Questo capitolo introduce brevemente i principi alla base di tale processo. Tratteremo inoltre i runlevel e la configurazione di un sistema SUSE tramite `sysconfig`.

7.1 Il processo di boot Linux

Il processo di boot in Linux si compone di diversi passaggi; illustreremo di seguito i vari stadi ed i componenti maggiormente coinvolti nel processo di avviamento.

1. **BIOS**

   Quando accendete il computer il BIOS (ingl. Basic Input Output System) inizializza schermo e tastiera ed esegue un test della memoria principale; il computer fino a questo punto non dispone di un supporto di memoria di massa. In seguito verranno lette le informazioni riguardanti la data attuale, l'ora e le periferiche più importanti dai valori CMOS (*CMOS setup*). Una volta rilevato il disco rigido e la sua geometria, il controllo passa dal BIOS al bootloader.

2. **Boot Loader**

   Durante questo passaggio viene caricato in memoria il primo settore di dati fisico di 512 byte ed il programma situato all'inizio di questo settore (il *boot loader*) assume il controllo del processo. La sequenza delle istruzioni eseguite tramite il bootloader determina l'ulteriore decorso del processo di boot. I primi 512 byte del primo hard disk vengono perciò anche chiamati *Master Boot Record* (MBR). Il boot loader cede il controllo al sistema operativo, nel nostro caso il kernel Linux. Per maggiori informazioni su GRUB ed il boot loader di Linux rimandiamo al capitolo 8 a pagina 177.

3. **Kernel ed initrd**

   Per cedere il controllo del processo al kernel, il boot loader carica nella memoria kernel e l'initial ramdisk (initrd). Il kernel di Linux contiene una opzione per caricare un piccolo file system nella ramdisk ed eseguire dei programmi prima che venga eseguito il mount del file system root vero e proprio. Il kernel decomprime quindi l'initrd e lo monta come file system root temporaneo. L'initrd contiene un sistema Linux minimale con un eseguibile chiamato linuxrc. Questo eseguibile viene eseguito prima che venga effettuato il mount del vero file system root. Se è data la possibilità, il kernel libera la memoria occupata da initrd ed avvia init dopo che linuxrc abbia terminato. Per maggiori informazioni su initrd si veda la sezione 7.1.1 nella pagina successiva.

4. **linuxrc**

   Questo programma esegue tutte le operazioni necessarie per il mount del file system vero e proprio, ossia mette a disposizione le funzionalità kernel per i file system richiesti e driver di dispositivi per controller di supporti di memoria di massa. Non appena l'effettivo file system root viene montato correttamente, linuxrc si ferma ed il kernel avvia il programma init. Per maggiori informazioni su linuxrc, si veda la sezione 7.1.2 nella pagina seguente.

5. **init**

   Il programma init gestisce il processo di boot nei vari stadi e offre tutta una serie di funzionalità; init viene descritto nella sezione 7.2 a pagina 163.

7.1.1 initrd

initrd è un piccolo file system (di solito compresso) che il kernel carica nella ramdisk e quindi monta come file system root temporaneo. initrd mette a disposizione un ambiente Linux minimale che permette l'esecuzione di determinati programmi prima che il file system vero e proprio venga montato. Sono le BIOS routine a caricare questo ambiente Linux minimale nella memoria, il quale non ha particolari requisiti hardware se non quello di richiedere abbastanza memoria. L'initrd contiene un eseguibile chiamato linuxrc che deve essere eseguito correttamente.

Prima che il file system root possa essere montato e il sistema operativo avviato, il kernel necessità dei corrispondenti driver per accedere al dispositivo sul quale si trova il file system root. Questi driver possono anche includere driver particolari per determinati dischi rigidi o anche driver di rete per consentire l'accesso a file system di rete (si veda nella pagina seguente). Il kernel deve inoltre contenere un codice richiesto per leggere il file system di initrd. I moduli richiesti per il file system root vengono caricati da linuxrc.

Potete creare un `initrd` servendovi dello script `mkinitrd`. In SUSE LINUX i moduli da caricare vengono stabiliti tramite la variabile `INITRD_MODULES` in `/etc/sysconfig/kernel`. Dopo l'installazione, questa variabile riceve automaticamente i valori giusti (il linuxrc dell'installazione sa quali moduli sono stati caricati). Degno di nota è il fatto che i moduli vengono caricati nella stessa sequenza in cui appaiono alla voce `INITRD_MODULES`. Ciò è particolarmente importante nel caso vengano usati più driver SCSI, poiché, altrimenti, cambierebbe la denominazione dei dischi rigidi. A rigor di logica, sarebbe sufficiente caricare

solo driver SCSI necessari all'accesso al file system root. Poiché, però, il caricamento automatico di ulteriori driver SCSI è problematico, vengono caricati tutti i driver SCSI necessari durante l'installazione tramite initrd.

Importante

Aggiornare initrd

Il boot loader carica initrd nello stesso modo del kernel. Non è necessario reinstallare GRUB dopo un update di initrd, poiché GRUB rileva il file corretto al boot

Importante

7.1.2 linuxrc

La funzione principale di linuxrc è quella di preparare il mount del file system root effettivo per potervi accedervi. In base alla configurazione del vostro sistema, linuxrc svolge le seguenti funzionalità.

Carica moduli del kernel Sempre in base al vostro assetto configurativo dell'hardware sono richiesti driver speciali per accedere alle componenti hardware del vostro sistema (prima di tutte il disco rigido). Per accedere il file system root definitivo, il kernel richiede che siano caricati i rispettivi driver per il file system.

Amministrare configurazioni RAID e LVM
Se il file system root si trova su software RAID o LVM, linuxrc imposta LVM o RAID in modo da consentire di accedere al file sytem root. Per delle indicazioni su RAID rimandiamo alla sezione 3.7 a pagina 105; per LVM vi è la sezione 3.6 a pagina 98.

Amministrare la configurazione di rete
Se utilizzate un file system root montato via rete (ad es. via NFS), linuxrc assicurerà che siano caricati i driver di rete richiesti e che siano impostati in modo da consentire l'accesso al file system root.

Se linuxrc viene invocato durante il processo di boot iniziale come parte del processo di installazione, le sue funzioni differiscono da quelle menzionate in precedenza:

Rilevare un mezzo di installazione All'inizio del processo di installazione, il programma di installazione di YaST carica dalla mezzo di installazione il kernel ed l'initrd. Il programma di installazione di YaST, che viene eseguito in un file system RAM, richiede delle informazioni sulla locazione attuale del mezzo di installazione per accedervi ed installare il sistema operativo.

Rilevamento hardware e carica dei moduli del kernel richiesti
Come già detto nella sezione 7.1.1 a pagina 161, il processo di boot si avvia con un minimo di driver che va bene per la maggior parte di configurazioni hardware. linuxrc avvia una scansione iniziale dell'hardware per determinare i driver richiesti per la vostra configurazione hardware. I valori rilevati vengono scritti sotto `INITRD_MODULES` in `/etc/sysconfig/kernel` per consentire nell'ulteriore decorso del processo di boot l'utilizzo di un initrd su misura. Durante il processo di installazione, linuxrc carica l'insieme di moduli richiesti.

Caricare il sistema di installazione o quello di salvataggio
Dopo il rilevamento dell'hardware e dopo che sono stati caricati i driver richiesti, linuxrc avvia il sistema di installazione, che contiene il programma di installazione YaST, oppure il sistema di salvataggio.

Avviare YaST Infine, linuxrc avvia YaST, che inizializza l'installazione dei pacchetti e la configurazione di sistema.

7.1.3 Ulteriori informazioni

Per maggiori dettagli si veda `/usr/src/linux/Documentation/ramdisk.txt`, `/usr/src/linux/Documentation/initrd.txt` e la pagina di man initrd(4) e mkinitrd(8).

7.2 Il programma init

Questo programma si usa definirlo padre di tutti i processi, ha il numero di processo 1 e inizializza il sistema nel modo richiesto. Tutti gli altri processi sono dei processi figlio di init. init ha un ruolo particolare, viene avviato direttamente dal kernel ed è immune al segnale 9, che fredda tutti i processi. Tutti gli altri programmi vengono avviati o direttamente da init o da un suo processo figlio.

init viene configurato centralmente nel file `/etc/inittab`, dove sono definiti i cosiddetti *runlevels* (si veda la sezione 7.3 nella pagina seguente). Inoltre questo

file specifica i demoni e servizi disponibili per ogni runlevel. In base alle registrazioni in `/etc/inittab`, init esegue diversi script. Per motivi di chiarezza, questi script risiedono nella directory `/etc/init.d`.

L'intero processo di avviamento e spegnimento del sistema viene gestito da init. In tal senso il kernel può essere considerato un processo in sottofondo con il compito di gestire tutti gli altri processi e di adeguare il tempo di CPU ed accesso all'hardware in base alle richieste dei programmi.

7.3 I runlevel

Linux dispone di diversi *runlevel* che definiscono i diversi stati del sistema. Il runlevel standard nel quale si carica il sistema viene stabilito nel file `/etc/inittab`, alla voce `initdefault`. Normalmente, il valore standard è `3` o `5` (si veda alla tabella 7.1 nella pagina successiva). Alternativamente, potrete impostare il runlevel desiderato durante il caricamento (ad esempio al prompt di boot); il kernel passa i parametri che non elabora a init.

Per passare ad un altro runlevel in un secondo momento, basta invocare `init` con il numero del runlevel del caso; solo l'amministratore del sistema può cambiare il livello di esecuzione del sistema. Ad esempio, con il comando `init 1` oppure `shutdownnow` si passa al *modo a utente singolo* (ingl. single user mode), che serve alla manutenzione ed amministrazione del sistema. Una volta che l'amministratore abbia completato il suo lavoro, immetterà `init 3` per avviare il sistema nel solito runlevel, nel quale girano tutti i programmi necessari al funzionamento del sistema e che permette di eseguire il login agli utenti. Con `init 0` o `shutdown -h now` potete spegnere il sistema e con `init 6` o `shutdown -r now` potete eseguire un reboot del sistema.

Importante

Runlevel 2 con partizione /usr/ montata via NFS

Il runlevel 2 non dovrebbe venir utilizzato su di un sistema, la cui partizione `/usr/` sia montata tramite NFS. La partizione `/usr/` contiene programmi necessari al funzionamento senza intoppi del sistema. Dato che il servizio NFS non è ancora disponibile nel runlevel 2 (modo multiutente locale senza rete remota), si verificherebbero delle notevoli restrizioni per quel che riguarda la funzionalità del vostro sistema.

Importante

Tabella 7.1: *Livelli di esecuzione disponibili*

Runlevel	Significato
0	Arresto del sistema
S	Modo utente singolo (ingl. single user mode); dal prompt di boot con la tastiera americana
1	Modo ad utente singolo (ingl. single user mode)
2	Modo multiutente locale senza rete remota (ingl. local multiuser without remote network; ad es. NFS)
3	Modo multiutente completo con rete (ingl.full multiuser with network)
4	Libero (ingl. not used)
5	Modo multiutente completo con rete e KDM (default), GDM o XDM
6	Riavvio del sistema

L'installazione standard di SUSE LINUX imposta di solito il runlevel `5` come standard, in modo che l'utente si possa immettere nel sistema direttamente tramite l'interfaccia grafica. Per cambiare il runlevel da `3` a `5`, accertatevi che il sistema X window sia già stato configurato correttamente; (si veda al capitolo 11 a pagina 223). Verificate se il sistema funziona nel modo desiderato, immettendo in seguito `init5`. In caso affermativo, con YaST potete impostare il runlevel di default su `5`.

Avvertimento

Modificare /etc/inittab

Degli errori in `/etc/inittab` potrebbero causare delle difficoltà all'avvio del sistema. Siate estremamente cauti nel modificare questo file e assicuratevi di conservare sempre una copia del file originale intatta. Per riparare dei danni, provate ad inserire, al prompt di boot il parametro `init=/bin/sh`, per poter caricare il sistema in una shell e, da lì, ricostruire il file originale. Inseguito rendete il vostro file system root accessibile in scrittura con `mount -o remount,rw /` e sostituite `cp` con la vostra copia di backup utilizzando il comando `cp`. Per evitare degli errori di file system, impostate il vostro file system root in modo di avere accesso in sola lettura, prima di eseguire un reboot tramite `mount -o remount,ro /`.

Avvertimento

7.4 Cambiare il runlevel

In genere quando si cambia runlevel questo significa che vengono eseguiti gli *script di arresto* del runlevel attuale che terminano diversi programmi in esecuzione del runlevel in questione. Allo stesso tempo, vengono eseguiti gli *script di inizializzazione* del nuovo runlevel e, nella maggioranza dei casi, avviati alcuni programmi. Per comprendere meglio questo processo, osserviamo l'esempio riportato nel quale eseguiamo il passaggio dal runlevel 3 al runlevel 5:

1. L'amministratore (`root`) ordina al processo init di cambiare runlevel, immettendo `init 5`.
2. init consulta il file di configurazione `/etc/inittab` e constata che lo script `/etc/init.d/rc` deve essere avviato con il nuovo runlevel come parametro.
3. Ora,`rc` esegue tutti gli script di arresto del runlevel attuale per i quali non vi sono script di avvio nel nuovo runlevel. Nel nostro esempio, si tratta degli script contenuti nella directory `/etc/init.d/rc3.d` (il runlevel precedente era `3`) e che iniziano con la lettera `K`. Il numero che segue la lettera `K` garantisce che venga mantenuta una determinata sequenza, dal momento che vi possono essere delle dipendenze tra i programmi.

4. Per ultimo, vengono eseguiti gli script di avvio del nuovo runlevel. Nel nostro esempio, questi script si trovano in `/etc/init.d/rc5.d` ed iniziano con S. Anche qui, si rispetta l'ordine stabilito dal numero che accompagna la lettera S.

Se passate nel runlevel in cui vi troviate già, init legge solo `/etc/inittab`, verifica la presenza di eventuali modifiche e, se necessario, adotta tutte le misure del caso (avviando, ad esempio, un `getty` su un'altra interfaccia).

7.5 Gli script init

Gli script in `/etc/init.d` si suddividono in due categorie:

Script che vengono avviati direttamente da init:
questi script vengono attivati non solo durante il caricamento del sistema, ma anche in caso di spegnimento improvviso del sistema (per mancanza d'elettricità o quando si preme la combinazione di tasti Ctrl-Alt-Canc). L'esecuzione degli script è definita in `/etc/inittab`.

Script che vengono avviati indirettamente da init:
si dà questo caso quando si esegue il passaggio da un runlevel all'altro, laddove, normalmente, il primo script `/etc/init.d/rc`, avvia gli altri nella sequenza corretta.

Tutti gli script si trovano in `/etc/init.d`, dove sono raccolti anche gli script per il passaggio da un runlevel all'altro. Gli script vengono lanciati attraverso un link simbolico da una delle sottodirectory tra `/etc/init.d/rc0.d` e `/etc/init.d/rc6.d`. In tal modo si ha maggior chiarezza e si evita di dover duplicare gli script per poterli usare, ad esempio, in runlevel differenti. Dal momento che ogni script può fungere sia da script d'avvio che di arresto, essi devono supportare sia il parametro `start` che `stop`. Inoltre, gli script accettano le opzioni `restart`, `reload`, `force-reload` e `status`; le funzioni delle opzioni sono riassunte nella tabella 7.2 nella pagina successiva. Gli script eseguiti direttamente da init non hanno questi link. Gli script vengono eseguiti indipendentemente dal runlevel all'occorrenza.

Tabella 7.2: *Rassegna delle opzioni degli script init*

Opzione	Significato
`start`	Avviare servizio: si potrà avviare anche un servizio già in esecuzione, anche se il risultato non cambia.
`stop`	Fermare servizio.
`restart`	Se il servizio è in esecuzione, fermarlo e riavviarlo; altrimenti, avviare servizio
`reload`	Ricarica la configurazione del servizio senza fermarlo e riavviarlo
`force-reload`	Ricarica la configurazione del servizio se il servizio supporta questa operazione; altrimenti come `restart`
`status`	Mostra lo stato attuale

I link che trovate nelle singole sottodirectory dei runlevel servono quindi solo alla allocazione dei singoli script a determinati runlevel. Per creare ed eliminare dei link, ci si serve di insserv (o di `/usr/lib/lsb/install_initd` che è uno script che invoca questo programma) durante l'installazione o disinstallazione dei pacchetti del caso; si veda la pagina di man di insserv(8) per maggiori dettagli. Segue una breve introduzione per gli script di caricamente, di arresto e dello script che coordina questo processo.

`boot` Viene eseguito all' avvio del sistema ed avviato direttamente da init. Non dipende dal runlevel di default e viene eseguito soltanto una volta: essenzialmente, vengono montati i file system `proc` e `pts`, e attivato blogd (ingl. "Boot Logging Daemon"), quindi nel caso dell'installazione di un nuovo sistema o dopo un'aggiornamento, viene inizializzata una configurazione di base.

blogd è un cosiddetto demone che viene inizializzato dallo script boot *e* rc prima di tutti gli altri, e dopo aver svolto la sua funzione (p.es. invocare gli sottoscript) viene terminato. Questo demone scrive i propri messaggi nel file di log `/var/log/boot.msg`, se `/var` è stata montata con accesso in lettura e scrittura, altrimenti memorizza temporaneamente nel buffer tutti i dati visualizzati sullo schermo, finché `/var` non venga montata con accesso in lettura e scrittura. Per ulteriori informazioni su blogd consultate la relativa pagina di manuale blogd(8).

Lo script `boot` ha il compito di inizializzare tutti gli script in `/etc/init.d/boot.d` che cominciano con la lettera `S`. Si esegue una verifica dei file system, si eliminano tutti i file superflui sotto `/var/lock` e viene configurata la rete per il dispositivo In caso di errori gravi durante la verifica e riparazione automatica dei file system, l'amministratore del sistema dovrà inserire la password di root e risolvere manualmente il problema. Alla fine, viene eseguito lo script `boot.local`.

`boot.local` Qui potete inserire dei comandi che desideriate eseguire al caricamento del sistema, prima che il sistema entri in uno dei runlevel. Questa funzione può essere paragonata all'`AUTOEXEC.BAT`.

`boot.setup` Impostazioni fondamentali da eseguire durante il passaggio dal modo a utente singolo ad un altro runlevel. Qui vengono caricate la mappatura della tastiera e la configurazione della console.

`halt` Questo script viene eseguito solo quando si entra nel runlevel 0 o 6. Viene avviato sotto il nome `halt` o `reboot`. A seconda del modo in cui viene lanciato `halt`, si ha il riavvio o il spegnimento del sistema.

`rc` Il primo script della serie ad essere avviato quando si effettua il passaggio tra un runlevel e l'altro. Esso esegue gli script di arresto del runlevel attuale e quelli di avvio del runlevel nuovo.

7.5.1 Aggiungere script di inizializzazione

Potete anche aggiungere degli script di inizializzazione vostri. Se avete delle domande sul formato, denominazione e struttura degli script di inizializzazione seguite le indicazioni della bozza dell'LSB e quelle riportate nelle pagine di manuale init(8), init.d(7) e insserv(8). In questo contesto sono di sicuro interesse anche le pagine di manuale startproc(8) e killproc(8).

Avvertimento

Generare propri script init

Degli errori negli script di inizializzazione possono bloccare l'intero sistema. Siate pertanto molto cauti quando generate degli script e verificatene il corretto funzionamento prima di utilizzarli nel modo multiutente. Per informazioni di base sull'uso degli script di inizializzazione dei runlevel, consultate la sezione 7.3 a pagina 164.

Avvertimento

Se per un vostro programma o un vostro servizio create uno script di inizializzazione, utilizzate come modello il file `/etc/init.d/skeleton`. Salvate questo file con il nuovo nome ed editate la designazione dei nomi di programma o di file e percorsi, e aggiungete all'occorrenza proprie sezioni di script necessarie ad eseguire correttamente il processo di inizializzazione.

Editate il blocco obbligatorio `INIT INFO` all'inizio del file, si veda all'esempio 7.1 in questa pagina.

Esempio 7.1: *Un INIT INFO minimale*

```
### 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
```

Nel primo rigo dell'intestazione `INFO` indicate dopo `Provides:` il nome del programma o servizio che deve essere amministrato da questo script di inizializzazione. `Required-Start:` e `Required-Stop:` contengono i servizi che devono essere avviati o terminati prima di lanciare o terminare il servizio o programma in questione. Questi dati vengono processati per ottenere la sequenza degli script di inizializzazione e di arresto nelle directory dei runlevel. Indicate i runlevel nei quali la vostra applicazione debba essere avviata o terminata in modo automatico accanto a `Default-Start:` e `Default-Stop:`. Infine inserite una breve descrizione della vostra applicazione accanto a `Description:`.

Con il comando `insserv <nome del nuovo script>` create i link che da `/etc/init.d/` puntano verso le relative directory dei runlevel (`/etc/init.d/rc?.d/`). insserv analizza automaticamente le indicazioni dell'intestazione dello script di inizializzazione e archivia i link per gli script di avvio e di arresto nelle relative directory dei runlevel. La sequenza di esecuzione corretta degli script di avvio e di arresto, all'interno di un runlevel, viene garantita da insserv sempre in base alla numerazione degli script. Come strumento di configurazione grafico per la creazione dei link avete a vostra disposizione l'editor dei runlevel di YaST; si veda la sezione 7.6 a fronte.

Se volete integrare nei vostri runlevel uno script che si trova già sotto `/etc/init.d/` dovete creare - tramite insserv o l'editor dei runlevel di YaST- dei link

che puntano alle relative directory dei runlevel ed abilitare il servizio. Al prossimo avvio del sistema verranno applicate le vostre modifiche e lanciato in modo automatico il nuovo servizio.

Non settate questi link manualmente, degli errori nel blocco `INFO`, compromettono il corretto funzionamento di `insserv`.

7.6 Editor dei runlevel

Dopo l'avvio di questo modulo verrà visualizzata una maschera iniziale che mostra tutti i servizi disponibili e il loro stato di abilitazione. Tramite i radio bottoni selezionate tra 'Modo semplice' o 'Modo per esperti'. Di default è selezionato 'Modo semplice' visto che si rivela essere sufficiente per la maggior parte dei casi. Nella tabella vedete elencati in ordine alfabetico tutti i servizi e demoni del vostro sistema. Sulla sinistra vedete i nomi dei servizi, al centro se sono abilitati o meno e sulla destra avete una breve descrizione. In basso vi viene mostrata una descrizione dettagliata del servizio attualmente selezionato. Per abilitare un servizio dovete selezionarlo nella tabella e fare clic su 'Abilita'. Per disabilitare dei servizi procedete in modo analogo.

Se volete intervenire in modo mirato su di un runlevel, per esempio volete avviare o terminare un determinato servizio di sistema, oppure cambiare il runlevel di default, selezionate il radio bottone 'Modo per esperti'. In questa maschera vedete per prima cosa il runlevel di default attuale che viene caricato all'avvio del vostro sistema. In SUSE LINUX di solito si tratta del runlevel 5 (Modo multiutente completo con rete e XDM). Un altro runlevel appropriato sarebbe p.es. il runlevel 3 (Modo multiutente completo con rete).

A questo punto YaST vi permette di impostare un altro runlevel di default; cfr. la tabella tabella 7.1 a pagina 165. I servizi e demoni si abilitano o disabilitano in questa tabella che vi offre delle informazioni riguardanti i servizi e demoni disponibili, il loro stato di abilitazione e per quali runlevel sono abilitati. Marcando una riga con un clic del mouse, potete attivare le caselle dei runlevel 'B', '0', '1', '2', '3', '5', '6' e 'S' e così stabilire per quali runlevel si debba attivare il relativo servizio o demone. Il runlevel 4 non è definito e resta a disposizione dell'utente per eventuali impostazioni proprie. Proprio sotto la lista viene mostrata una breve descrizione del servizio o demone selezionato.

Con 'Avviare/Fermare/Aggiornare', decidete se utilizzare un determinato servizio. Con 'Aggiorna lo stato', potete verificare lo stato attuale, nel caso in cui

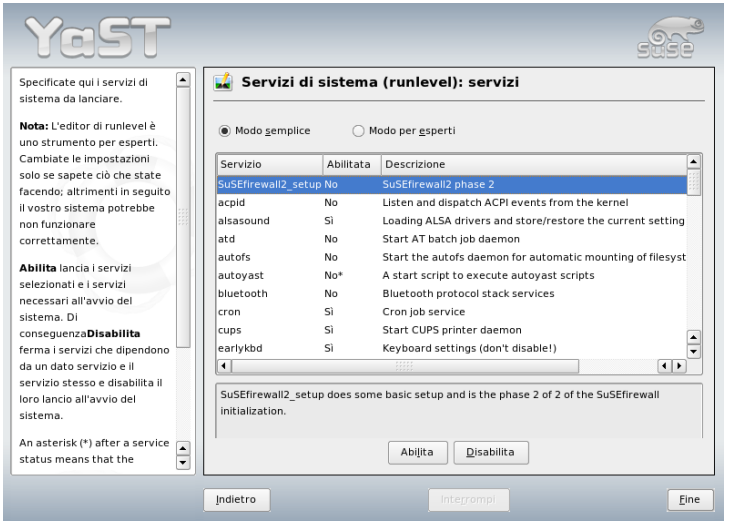

Figura 7.1: *Editor dei runlevel*

non sia già stato fatto automaticamente. Con 'Applica/Ripristinare' decide se applicare le impostazioni fatte o riportare il sistema allo stato dopo l'installazione. Con 'Fine' salvate la configurazione del sistema.

Avvertimento

Modificare le impostazioni dei runlevel

Un'impostazione erronea dei servizi di sistema e dei runlevel può compromettere seriamente la funzionalità del vostro sistema. Prima di modificare delle impostazioni, vi preghiamo quindi di informarvi sulle possibili conseguenze per quanto concerne la funzionalità del vostro sistema.

Avvertimento

7.7 SuSEconfig e /etc/sysconfig

Principalmente la configurazione di viene realizzata tramite i file di configurazione che trovate sotto `/etc/sysconfig`. Nelle versioni precedenti di SUSE LINUX si utilizzava a riguardo il file `/etc/rc.config` che è diventato ormai obsoleto. Quando installate questo file non viene più generato. La configurazione del sistema si realizza adesso tramite i file che si trovano sotto `/etc/sysconfig`. Se eseguite un aggiornamento e se vi è già sul vostro sistema il file `/etc/rc.config`, chiaramente non verrà cancellato.

Ogni volta che modificate i suddetti file, in seguito dovete anche lanciare SuSEconfig, per assicurare che le nuove impostazioni vengano applicate. Se usate l'editor sysconfig di YaST, se ne occuperà lui ad avviare automaticamente SuSEconfig che aggiornerà tutti i file interessati.

Questo approccio rende possibile apportare delle rilevanti modifiche alla configurazione del sistema senza doverlo riavviare. Nel caso di modifiche di ampia portata comunque, a volte tuttavia è necessario riavviare alcuni programmi per rendere effettive le modifiche.

Se modificate la configurazione di rete immettendo i comandi `rcnetwork stop` e `rcnetwork start`, riavviati i programmi di rete appena modificati.

Per configurare il sistema vi consigliamo di procedere come segue:

1. Portate il sistema nel *modo utente singolo*, ovvero (runlevel 1) con: `init 1`
2. Modificate i file di configurazione. Servitevi a riguardo di un editor di testo o, meglio, dell'editor sysconfig di YaST cfr. la sezione 7.8 nella pagina seguente.

Avvertimento

Editare manualmente la configurazione del sistema

Se *non* editate i file di configurazione che trovate sotto `/etc/sysconfig` con YaST un parametro vuoto va scritto sotto forma di due virgolette susseguenti (ad esempio `KEYTABLE=""`) ed i parametri che contengono degli spazi devono avere le virgolette all'inizio e alla fine del parametro. Le variabili composte da una sola parola non necessitano delle virgolette.

Avvertimento

3. Eseguite `SuSEconfig` per rendere effettive le modifiche fatte. Questo avverrà automaticamente, se avete usato YaST per impostare il runlevel.

4. Riportate il sistema al runlevel precedente tramite `init 3` (nell'esempio, `3`):

Questa procedura si rende chiaramente necessaria solo nel caso di modifiche di ampia portata (ad esempio, la configurazione di rete). In casi più semplici non è neanche necessario che l'amministratore passi al "modo utente singolo"; tuttavia, assicuratevi che tutti i programmi interessati dalle modifiche apportate vengano riavviati.

Suggerimento

Potete disattivare la configurazione automatica tramite SuSEconfig *globalmente* impostando la variabile `ENABLE_SUSECONFIG` in `/etc/sysconfig/suseconfig` su `no`. Per poter usufruire del supporto all' installazione, la variabile `ENABLE_SUSECONFIG` dovrà tuttavia essere impostata su `yes`. Potete disattivare in modo mirato anche solo determinate sezioni della configurazione automatica.

Suggerimento

7.8 L'editor sysconfig di YaST

Nella directory`/etc/sysconfig`, troverete tutti i file contenenti le impostazioni principali per SUSE LINUX. L'editor sysconfig vi presenta tutte le possibilità di impostazione. I valori possono essere modificati e poi inseriti nei singoli file di configurazione. Le modifiche apportate manualmente, tuttavia di solito non sono necessarie, dal momento che i file vengono aggiornati automaticamente ogni volta che venga installato un pacchetto o impostato un servizio.

Avvertimento

Modificare i file /etc/sysconfig/*

Le vostre modifiche apportate sotto `/etc/sysconfig/*` incidono profondamente su tutto il sistema. Prima di apportare delle modifiche, chiarite quali potrebbero essere le possibili conseguenze, per non compromettere il funzionamento del vostro sistema. Tutta una serie di variabili sysconfig dei file sotto `/etc/sysconfig/` sono accompagnate da commenti che ne illustrano la funzione.

Avvertimento

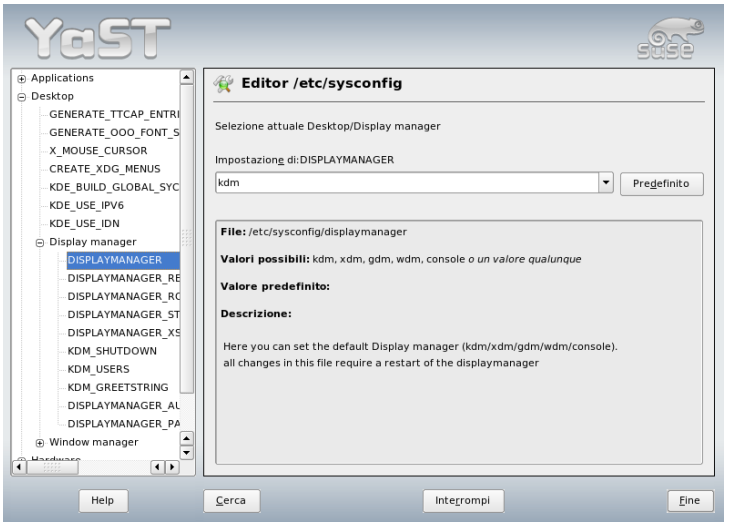

Figura 7.2: *Configurazione del sistema tramite l'editor sysconfig*

L'editor sysconfig di YaST si avvia con una maschera tripartita. A sinistra potete selezionare le variabili da configurare disposte in una struttura ad albero. Non appena selezionate una variabile sulla destra compaiono il nome della selezione e le impostazioni attualmente valide per la variabile. Sotto le variabili trovate una breve descrizione, i possibili valori che possono assumere, l'impostazione di default nonché il file in cui viene salvata la variabile selezionata. Inoltre vedete quale script di configurazione viene lanciato in caso di modifiche apportate a

questa variabile e quale servizio viene riavviato. YaST vi chiede di confermare le vostre modifiche e vi informa, quali script saranno eseguiti quando uscirete da questo modulo dopo aver premuto su 'Fine'. Potete anche saltare l'avvio di determinati servizi e script qualora lo riteneste opportuno.

Il boot manager

In questo capitolo descriveremo come configurare GRUB, il boot loader utilizzato con SUSE LINUX. Il rispettivo modulo YaST vi permette di eseguire comodamente tutte le impostazioni necessarie. Se non avete ancora dimestichezza con il processo di boot sotto Linux, proseguite con la lettura dei seguenti paragrafi per apprendere le nozioni teoretiche di base di questa tematica. Il capitolo si chiude con eventuali difficoltà che potrebbero verificarsi con GRUB e delle indicazioni sul modo di risolverle.

Questo capitolo è dedicato alla gestione del processo di boot ed alla configurazione del boot loader GRUB. Il processo di boot nel suo insieme viene illustrato in capitolo 7 a pagina 159. Un boot loader funge da interfaccia tra la macchina (BIOS) ed il sistema operativo (SUSE LINUX). La configurazione del boot loader determina il sistema operativo da avviare e le relative opzioni a disposizione.

Ecco la terminologia usata nel presente capitolo:

Master Boot Record La struttura dell'MBR è stabilita da una convenzione estesa a tutti i sistemi operativi. I primi 446 byte sono riservati al codice del programma. I successivi 64 byte offrono lo spazio per la tabella delle partizioni contenente fino a 4 registrazioni; si veda la sezione sezione Tipi di partizioni a pagina 11. La tabella delle partizioni continene delle informazioni sul partizionamento del disco rigido e tipo di file system. Al sistema operativo occorre questa tabella per indirizzare il disco rigido. Gli ultimi 2 byte devono contenere un "numero magico" (AA55): un MBR con un numero diverso viene considerato non valido dal BIOS e da tutti i sistemi operativi da PC.

Settori di boot I settori di boot sono i primi settori delle partizioni del disco rigido, fatta eccezione per le partizioni estese che sono solo un "contenitore" di altre partizioni. I settori di boot hanno un volume di 512 byte e sono atti a contenere un codice in grado di inizializzare un sistema operativo che si trova su questa partizione: questo vale anche per settori di boot di partizioni DOS, Windows o OS/2 formatate (che contengono inoltre dati fondamentali del file system). Al contrario dei suddetti settori di boot, quelli delle partizioni Linux – anche dopo la creazione di un file system – sono all'inizio vuoti (!). Perciò una partizione Linux *non è avviabile da sé,* anche se contiene un kernel e un file system root valido. Un settore di boot con un codice valido per l'avvio del sistema deve avere negli ultimi 2 byte lo stesso contrassegno "magico" dell'MBR (AA55).

8.1 Boot management

Il caso più semplice in tema di "boot management" si ha quando su un sistema è installato solamente un sistema operativo, come descritto sopra. Non appena si installano diversi sistemi operativi si hanno le seguenti possibilità:

Avviare il sistema aggiuntivo da un supporto esterno
Un sistema operativo viene caricato dal disco, gli altri tramite un boot manager, installato su un supporto esterno (ad es. dischetto, CD, chiave USB); visto che GRUB è in grado di caricare tutti gli altri sistemi operativi non è necessario avere un bootloader esterno.

Installare un boot manager nell'MBR
Un boot manager permette di avere su un computer contemporaneamente più sistemi operativi e di usarli in alternanza. L'utente sceglie il sistema da caricare durante all'avvio del computer; per passare da un sistema operativo all'altro si deve riavviare il computer. La premessa è comunque che il boot manager armonizzi bene con i diversi sistemi operativi. Il boot manager di SUSE LINUX carica tutti i sistemi operativi di maggior diffusione. Di default, SUSE LINUX installa quindi il boot manager prescelto nell'MBR, se non modificate questa impostazione durante il processo di installazione.

8.2 Selezionare il bootloader

Di default, SUSE LINUX utilizza il boot loader GRUB. In casi eccezionali comunque e con installazioni di software o hardware particolari bisogna ripiegare su LILO. Se eseguite l'update di una versione SUSE LINUX precedente che utilizzava LILO, allora LILO verrà nuovamente installato. Se eseguite l'installazione per la prima volta verrà installato GRUB, tranne per i casi in cui la partizione root viene installata sui seguenti sistemi :

- Controller RAID che dipende dalla CPU (come ad es. tanti controller Promise o Highpoint)
- Software-Raid
- LVM

Per reperire delle informazioni sull'installazione e configurazione di LILO consultate la nostra banca dati di supporto, eseguendo un ricerca di articoli che contengono la parola chiave *LILO*.

8.3 Boot con GRUB

GRUB (Grand Unified Bootloader) presenta due livelli; il primo livello (stage1) di 512 byte viene scritto nell' MBR o nel settore di boot della partizione o su dischetto. Il secondo livello più ampio (stage2) viene caricato in seguito e contiene il codice di programma in sé. L'unico compito del primo livello di consiste nel caricare il secondo livello del boot loader.

stage2 può accedere ai file system. Al momento vengono supportati Ext2, Ext3, ReiserFS, JFS, XFS, MINIX e il DOS FAT FS di Windows. Con delle restrizioni vengono supportati JFS XFS ed anche UFS/FFS utilizzato da sistemi BSD. A partire dalla versione 0.95 è anche in grado di effettuare il boot secondo la specificazione "El Torito" da CD o DVD con un file system standard ISO 9660. GRUB è in grado di accedere a file system di dispositivi a disco Bios (dischetti o dischi rigidi rilevati dal BIOS, lettori di CD e DVD) prima del boot, motivo per cui modifiche apportate al file di configurazione di GRUB (`menu.lst`) non significano più dover eseguire una reinstallazione del boot manager. All'avvio GRUB ricarica il file menu e i percorsi attuali nonché le informazioni sul partizionamento riguardanti il kernel o la ramdisk iniziale (`initrd`) e trova da sé questi file.

La configurazione di GRUB avviene attraverso tre file, illustrati di seguito:

`/boot/grub/menu.lst` Il file contiene le indicazioni su partizioni o sistemi operativi avviabili da GRUB. Se mancano queste indicazioni non è possibile passare il controllo del sistema al sistema operativo.

`/boot/grub/device.map` Questo file "converte" nomi di dispositivi dalla annotazione GRUB e BIOS in quella Linux.

`/etc/grub.conf` Questo file indica i parametri e opzioni richiesti dalla GRUB shell per una installazione corretta del bootloader.

GRUB si lascia gestire in vario modo. Le voci di boot di una configurazione già esistente possono essere selezionate tramite un menu grafico (splashscreen). La configurazione viene caricata dal file `menu.lst`.

GRUB presenta il grande vantaggio di consentire di modificare comodamente tutti i parametri di boot *prima* del boot. Se ad esempio avete fatto un errore editando il file menu, in questo modo potrete provvedere a correggerlo. Inoltre, potete immettere dei comandi di boot interattivamente tramite una sorta di prompt (si veda la sezione sezione Modificare le voci di menu durante il processo di boot a pagina 185). GRUB consente inoltre ancor prima del boot di individuare

la locazione del kernel e di `initrd`. In tal modo caricate anche sistemi operativi sprovvisti di una voce nel menu di boot.

Infine, il sistema installato include una GRUB *shell*, una emulazione di GRUB. La GRUB shell serve ad installare o testare delle nuove impostazioni prima di applicarle effettivamente (si veda la sezione sezione 8.3.4 a pagina 188).

8.3.1 Il menu di boot di GRUB

Lo splash screen grafico con il menu di boot viene configurato tramite il file di configurazione di `/boot/grub/menu.lst` che contiene tutte le informazioni sulle partizioni o sistemi operativi che possono essere caricati attraverso il menu.

Ad ogni avvio di sistema GRUB carica i file menu del file system. Dunque non bisogna aggiornare GRUB dopo aver modificato il file — utilizzate semplicemente il modulo YaST per la configurazione del bootloader (si veda la sezione sezione 8.4 a pagina 190).

Il file menu contiene dei comandi. La sintassi è molto semplice. Ogni file contiene un comando seguito da parametri opzionali separati da spazi come nella shell. Per motivi che potremmo definire storici è possibile anteporre il segno d'uguaglianza (=) al primo parametro di alcuni comandi. I commenti vengono introdotti dal carattere (#).

Ai fini dell'identificazione delle registrazioni di menu nella tavola sinottica dei menu, ad ogni registrazione dovete dare un nome o un `title`. Il testo che segue la parola chiave `title` verrà visualizzato, spazi inclusi, quale opzione da selezionare. Tutti i comandi fino al prossimo `title` vengono eseguiti dopo la selezione della registrazione del menu.

Il caso più semplice è rappresentato da un collegamento in serie di boot loader di diversi sistemi operativi. Il comando è `chainloader` e l'argomento è di solito il blocco di boot di un'altra partizione nella annotazioni dei blocchi di GRUB per esempio:

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

I nomi dei dispositivi in GRUB vengono spiegati nella sezione sezione Denominazioni dei dischi rigidi e partizioni nella pagina seguente. Nell'esempio di sopra viene specificato il primo blocco della quarta partizione del primo hard disk.

Con il comando `kernel` viene specificata una immagine del kernel. Il primo argomento è il percorso all'immagine del kernel su una partizione. Gli altri argomenti vengono passati al kernel tramite la linea di comando.

Se il kernel è sprovvisto dei driver necessari per accedere alla partizione root, allora dovete ricorrere ad `initrd`. Si tratta di un comando GRUB a sè stante che ha come solo argomento il percorso del file `initrd`. Dato che l'indirizzo di caricamento di `initrd` viene scritto nell'immagine del kernel già caricata, il comando `initrd` deve seguire al comando `kernel`.

Il comando `root` semplifica la specificazione dei file del kernel e file initrd. `root` ha come unico argomento un dispositivo GRUB oppure una partizione su un tale dispositivo. A tutti i percorsi del kernel, di `initrd` o di altri file senza una esplicita indicazione di un dispositivo viene preposto questo dispositivo fino al prossimo comando `root`. Questo comando non è incluso in un `menu.lst` generato durante l'installazione. Esso semplifica meramente le modifiche apportate manualmente

Alla fine di ogni registrazione di menu vi è implicitamente il comando `boot`, in modo che non debba essere scritto nel file di menu. Per un avvio interattivo con GRUB, il comando `boot` deve essere aggiunto alla fine. `boot` non ha argomenti, esegue semplicemente l'immagine del kernel caricata o il chain loader indicato.

Dopo aver compilato tutte le registrazioni di menu dovete stabilire una registrazione come `default`, altrimenti verrà utilizzata la prima registrazione (`0`). Potete anche stabilire un timeout in secondi prima che ciò avvenga. `timeout` e `default` di solito vengono scritti davanti alle registrazioni di menu. Un file esempio con relative spiegazioni si trova nella sezione sezione Esempio di un file menu nella pagina successiva.

Denominazioni dei dischi rigidi e partizioni

GRUB utilizza una convenzione diversa per designare dischi rigidi e partizioni rispetto ai soliti dispositivi Linux (p.es. `/dev/hda1`). Ad esempio la prima partizione del primo disco rigido è `hd0,0`. Su una sistema desktopo con un disco rigido connesso come master primario il nome di dispositivo Linux sarebbe `/dev/hda1`.

Le quattro possibili partizioni primarie hanno i numeri di partizione da `0` a `3`. `4` è la prima partizione logica:

```
(hd0,0)   prima partizione primaria sul primo disco rigido
(hd0,1)   seconda partizione primaria
(hd0,2)   terza partizione primaria
(hd0,3)   quarta partizione primaria (spesso partizione estesa)
(hd0,4)   prima partizione logica
(hd0,5)   seconda partizione logica
```

GRUB non distingue tra dispositivi IDE, SCSI o RAID. Tutti i dischi rigidi rilevati dal BIOS o da altri controller, vengono numerati nella sequenza di boot preimpostata nel BIOS.

Anche con GRUB si ha il fatto che nomi di dispositivi Linux non si lasciano correlare in modo chiaro ai nomi di dispositivi BIOS. GRUB utilizza un algoritmo per generare tale correlazione. Comunque, GRUB archivia questa correlazione nel file `device.map` che potete editare. Per ulteriori informazioni su `device.map` consultate la sezione sezione 8.3.2 a pagina 187.

Un percorso GRUB completo consiste di un nome di dispositivo scritto tra parentesi e il percorso del file nel file system sulla partizione indicata. Il percorso inizia con uno slash. Ecco un esempio per un kernel atto al boot su di un sistema con un solo disco rigido IDE e con Linux sulla prima partizione:

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

Esempio di un file menu

Per meglio comprendere la struttura di un file menu presentiamo un breve esempio. Questa installazione esempio contiene una partizione di boot Linux sotto `/dev/hda5`, una partizione root sotto `/dev/hda7` ed una installazione Windows sotto `/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
```

Il primo blocco riguarda la configurazione dello splash screen:

gfxmenu (hd0,4)/message L'immagine dello sfondo si trova su `/dev/hda5` e porta il nome `message`

color white/green black/light-gray Lo schema cromatico: bianco (primo piano), blu (sfondo), nero (selezione) e grigio chiaro (sfondo della selezione). Questo schema cromatico non incide sullo splash screen, ma in un primo momento sul menu di GRUB che potete modificare in cui entrate dopo essere uscito dallo splashscreen con Esc.

default 0 La prima voce di menu con `title linux` deve essere avviata di default.

timeout 8 Trascorsi otto secondo senza un intervento da parte dell'utente, esegue il boot in modo automatico.

Il secondo blocco più esteso elenca i sistemi operativi da poter caricare. Le sezioni per i singoli sistemi operativi sono introdotte da `title`.

- La prima registrazione (`title linux`) avvia SUSE LINUX. Il kernel (`vmlinuz`) si trova sul primo disco rigido nella prima partizione logica (in questo caso la partizione di boot). Parametri del kernel come ad esempio l'indicazione della partizione root, il modo VGA etc. vengono aggiunti qui. L'indicazione della partizione root deve seguire lo schema Linux (`/dev/hda7/`) visto che questa informazione è destinata al kernel e non riguarda GRUB. `initrd` si trova anche sulla prima partizione logica del primo disco rigido.
- La seconda registrazione carica Windows. Windows viene caricato dalla prima partizione del primo disco rigido (`hd0,0`). Con `chainloader +1` GRUB carica ed esegue il primo settore della partizione indicata.
- La prossima sezione serve ad eseguire il boot dal dischetto, senza dover intervenire sul BIOS.
- Con l'opzione di boot `failsafe` potete lanciare Linux con una determinata scelta di parametri del kernel che consentono di caricare Linux anche su sistemi problematici.

Il file menu può essere modificato in qualsiasi momento e GRUB lo caricherà automaticamente al prossimo boot. Potete editare questo file con il vostro editor preferito o con YaST in modo permanente. Potete anche apportare delle modifiche temporanee tramite la funzione edit di GRUB. (si veda la sezione sezione Modificare le voci di menu durante il processo di boot in questa pagina).

Modificare le voci di menu durante il processo di boot

Nel menu di boot grafico di GRUB potete selezionare tramite i tasti cursore il sistema operativo da caricare tra quelli disponibili. Se selezionate un sistema Linux al prompt di boot – come già per – potete immettere propri parametri di boot. Se premete (Esc) e uscite dallo splash screen dopo aver immesso (e) (edit) potete editare direttamente in modo mirato le singole voci di menu. Le modifiche fatte in questa maniera sono di natura temporanea, al prossimo boot scompariranno.

Importante

Mappatura della tastiera durante il boot

Tenete presente che al boot si ha la mappatura americana dei tasti, di conseguenza i caratteri speciali sono scambiati.

Importante

Dopo aver attivato il modo edit, selezionate tramite i tasti cursore la voce di menu di cui modificare la configurazione. Per poter editare la configurazione immettete ancora una volta (e). In tal modo potete correggere indicazioni errate riguardanti le partizioni o i percorsi prima che si ripercuotono sul processo di boot. Con (Invio) uscite dal modo edit e tornate al menu da dove potete avviare tale voce con (b). Nel testo di assistenza nella parte inferiore vengono descritti altri possibili modi di intervenire.

Se volete rendere permanenti le opzioni di boot aprite come `root` il file `menu.lst` ed aggiungete ulteriori parametri di kernel dopo uno spazio alla riga esistente:

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

GRUB assume i nuovi parametri automaticamente al prossimo boot. Come alternativa potete anche invocare il modulo del boot loader di YaST. Anche qui basta aggiungere ulteriori parametri alla riga esistente separati da uno spazio.

Le wild card e la selezione del kernel di boot

Soprattuto quando sviluppate o utilizzate dei kernel personalizzati vi tocca modificare le voci in `menu.lst` o modificare la linea di comando in modo da riflettere i nomi attuali del kernel e file initrd. Potete semplficare il tutto utilizzando delle *wild cards* per aggiornare l'elenco kernel di GRUB in modo dinamico. Tutte le immagine di kernel che soddisfano determinate condizioni vengono aggiunte all'elenco delle immagini avviabili. Tenete presente che non potremo offrire del servizio di supporto per questa funzionalità.

Abilitate l'opzione delle wild card aggiungendo un'ulteriore voce di menu in `menu.lst`. Tutte le immagini di kernel ed initrd devono avere lo stesso nome di base ed un identificatore che esegue la correlazione tra kernel e il rispettivo initrd. Ecco un esempio:

```
initrd-default
initrd-test
vmlinuz-default
vmlinuz-test
```

In questo caso potete aggiungere entrambi le immagini di boot in una configurazione GRUB. Per avere le voci di menu `linux-default` e `linux-test` occorre la seguente registrazione in `menu.lst`:

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

Nel nostro esempio, GRUB cerca nella partizione (hd0,4) delle registrazioni che corrispondono alla wild card. Queste registrazioni vengono utilizzate per generare le nuove voci di menu di GRUB. Nel precedente esempio, GRUB si comporterebbe come se esistesse la seguente registrazione in `menu.lst`:

```
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
```

Se vi sono dei nomi file non consistenti o se manca un file tipo l'immagine initrd potranno sorgere delle difficoltà.

8.3.2 Il file device.map

Il file `device.map` contiene la correlazione dei nomi di dispositivo GRUB e di quelli Linux. Se avete un sistema misto con dischi rigidi IDE e SCSI, GRUB tenterà di rilevare la sequenza di boot in base ad un particolare procedimento. Le informazioni BIOS a riguardo non sono accessibili a GRUB. Il risultato di tale analisi viene archiviato da GRUB sotto `/boot/grub/device.map`. Ecco un file esempio `device.map` per un sistema esempio – partiamo dal presupposto che la sequenza di boot impostata nel BIOS prevede che i dischi IDE vengono rilevati prima di quelli SCSI:

```
(fd0)  /dev/fd0
(hd0)  /dev/hda
(hd1)  /dev/sda
```

Dato che la sequenza dei dischi rigidi IDE, SCSI ed altri tipi di dispositivi del genere dipende da una serie di fattori e Linux non ne rivela la correlazione, vi è la possibilità di impostare la sequenza manualmente in `device.map`. Se al prossimo boot del sistema si dovessero verificare delle difficoltà, controllate la sequenza di boot e cambiatela se necessario tramite la GRUB shell (si veda la sezione sezione 8.3.4 nella pagina seguente). Una volta caricato il sistema Linux, con il modulo del boot loader di YaST oppure con un editor di vostra preferenza potete modificare il file `device.map` in modo permanente.

Dopo avere apportato delle modifiche manualmente al file `device.map`, date il seguente comando per reinstallare GRUB. Con questo comando vengono letti inoltre il file `device.map` ed eseguiti i comandi contenuti in `grub.conf`:

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

8.3.3 Il file /etc/grub.conf

Il terzo importante file di configurazione di GRUB accanto a `menu.lst` e `device.map` è `/etc/grub.conf`. Qui trovate i parametri e le opzioni richiesti dal comando `grub` per installare correttamente il boot loader:

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

Il significato delle singole registrazioni:

root (hd0,4) Con questo comando si istruisce GRUB a riferirsi per i seguenti comandi alla prima partizione logica del primo disco rigido, dove trova i file di boot.

install `parametro` Il comando `grub` deve essere lanciato con il parametro `install`. `stage1` come primo livello del boot loader deve essere installato nell'MBR del primo disco rigido (`/grub/stage1 d (hd0)`). `stage2` deve essere caricato nell'indirizzo di memoria 0x8000 (`/grub/stage2 0x8000`). L'ultima registrazione `(hd0,4)/grub/menu.lst` indica a `grub` dove trovare il file menu.

8.3.4 La GRUB shell

Esistono due versioni di GRUB: una volta come boot loader e una volta come normale programma Linux che trovate sotto `/usr/sbin/grub`. Questo programma viene chiamato *GRUB shell*. La funzionalità di installare GRUB quale boot loader su un disco rigido o dischetto è integrata direttamente in GRUB sotto forma del comando `install` o `setup`. In tal modo è disponibile nella GRUB shell, una volta caricato Linux.

Questi comandi sono comunque già disponibili *durante* il processo di boot senza che sia necessario che Linux sia già in esecuzione. Questo semplifica il ripristino di un sistema difettoso non più avviabile, dato che è possibile aggirare il file di configurazione corrotto del bootloader tramite l'immissione manuale di parametri. L'immissione manuale di parametri in fase di boot permette inoltre di verificare nuove impostazioni senza mettere a repentaglio il funzionamento del sistema nativo. Immettete semplicemente il comando di configurazione a titolo di prova attenendovi alla sintassi di `menu.lst`; verificate la funzionalità dell'immissione senza andare a toccare il file di configurazione attuale e così evitate l'insorgere di eventuali difficoltà in fase di boot del sistema. Se ad esempio intendete testare un nuovo kernel, immettete il comando `kernel` con indicazione del percorso al nuovo kernel. Se il processo di boot non si svolge correttamente, potrete ricorrere al prossimo boot al `menu.lst` intatto. In tal modo l'interfaccia a riga di comando permette anche di avviare il sistema nonostante la presenza di un `menu.lst` corrotto, immettendo dei parametri corretti. Con il sistema in esecuzione reinserite i parametri corretti nel vostro `menu.lst`. Così il sistema è nuovamente avviabile.

Solo se la GRUB shell gira quale programma Linux (da invocare con `grub` come illustrato ad esempio nella sezione sezione 8.3.2 a pagina 187), entra in gioco l'algoritmo di correlazione dei nomi di dispositivo GRUB e Linux. Il programma legge il file `device.map`. Per maggiori dettagli si veda la sezione sezione 8.3.2 a pagina 187.

8.3.5 Impostare la boot password

GRUB consente di accedere ai file system già in fase di boot, ciò significa che si può accedere a dei file del vostro sistema Linux a cui - a sistema caricato - può accedere solo root. Impostando una password evitate che vi siano degli accessi a questi file in fase di boot. Potete proibire gli accessi al file system durante il boot ad utenti non autorizzati o proibire l'esecuzione di determinati sistemi operativi agli utenti.

Per impostare una boot password procedete come `root` nel modo seguente:

1. Immettete al root prompt `grub`.
2. Cifrate la password nella GRUB shell:

   ```
   grub> md5crypt
   Password: ****
   Encrypted: $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
   ```

3. Inserite il valore cifrato nella sezione globale del file `menu.lst`:

   ```
   gfxmenu (hd0,4)/message
   color white/blue black/light-gray
   default 0
   timeout 8
   password --md5 $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
   ```

   Adesso l'esecuzione di comandi in fase di boot è protetta, solo dopo aver immesso ⓟ e la password sarà possibile eseguire dei comandi. Continua ad essere comunque consentito agli utenti di lanciare un sistema operativo dal menu di boot.

4. Per escludere la possibilità di lanciare uno o diversi sistemi operativi dal menu di boot, immettete nel file `menu.lst` la voce `lock` per ogni sezione da proteggere con una password. Esempio:

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

Dopo un reboot del sistema e la selezione della voce Linux nel menu di boot si ha il seguente messaggio di errore:

```
Error 32: Must be authenticated
```

Premete (Invio) per giungere al menu ed in seguito (p) per ottenere un prompt per la password. Dopo aver immesso la password e premuto (Invio) viene caricato il sistema operativo selezionato (in questo caso Linux).

Importante

Boot password e splash screen

Se utilizzate una boot password per GRUB, non viene visualizzato il consueto splash screen.

Importante

8.4 La configurazione del boot loader con YaST

La maniera più semplice per configurare il boot loader in SUSE LINUX è tramite l'apposto modulo YaST. Aprite il centro di controllo di YaST e andate al modulo 'Sistema' → 'Configurazione boot loader', dove potrete modificare la configurazione del boot loader del vostro sistema (si veda la figura 8.1 nella pagina successiva).

8.4.1 La finestra principale

L'area di configurazione bianca si divide in tre colonne: a sinistra, sotto 'Modificato', vengono evidenziate le opzioni modificate che sono riportate della colonna centrale. I valori attuali si trovano nella colonna a destra. Per aggiungere una nuova opzione, cliccate sul pulsante 'Aggiungi'. Per modificare il valore di

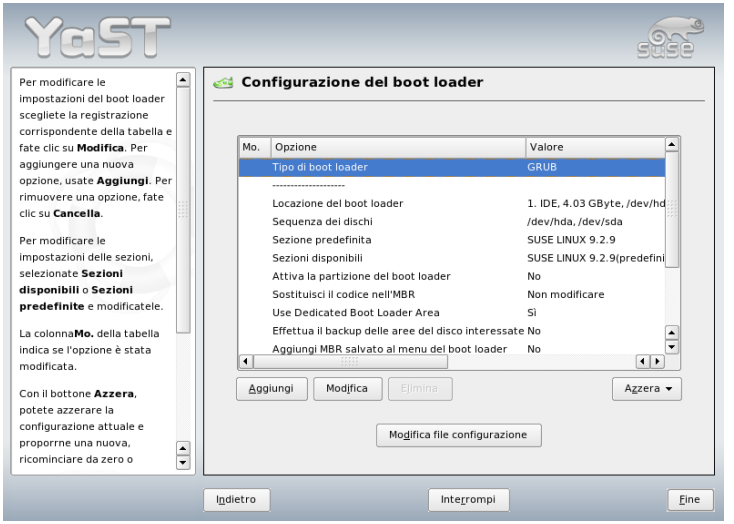

Figura 8.1: *La configurazione del boot loader con YaST*

una un'opzione, selezionatela e cliccate su 'Modifica'. Se desiderate disattivare un'opzione, selezionatela e cliccate su 'Elimina'.

Sotto la finestra di configurazione, trovate la casella combinata 'Azzera' con le seguenti opzioni:

Proponi nuova configurazione Il programma vi propone una nuova configurazione e, se trova una versione precedente di Linux o un altro sistema operativo su altre partizioni, li integra nel menu di caricamento. Tramite il menu potrete selezionare se caricare direttamente Linux o il suo vecchio boot loader. Nell'ultimo caso, compare un secondo menu.

Cominciare 'ex novo' La configurazione sarà determinata da voi, senza alcun suggerimento da parte di YaST.

Ricarica configurazione dal disco rigido
Se non siete soddisfatti delle vostre modifiche, potete ricaricare la vecchia configurazione dal disco rigido.

Proporre e aggiungere al menu di GRUB
Se vi è un altro sistema operativo o una versione precedente di Linux su

un'altra partizione, il menu conterrà un'opzione di caricamento per il nuovo SUSE LINUX, una per l'altro sistema e tutte le opzioni del menu del vecchio boot loader. Questo procedimento potrà richiedere un po' di tempo. Se utilizzate LILO questa possibilità non è data.

Ripristina MBR dal disco rigido In tal modo si ripristina l'MBR salvato sul disco rigido.

Al di sotto della combo box vi è il pulsante 'Modifica file di configurazione' che vi permette di modificare questi file in un editor. Cliccate su uno dei file della lista: il file verrà caricato in un editor e potrà essere modificato a piacimento. Per salvare le vostre modifiche, cliccate su 'OK'. Per uscire dalla configurazione del boot loader, selezionate 'Interrompi'. Con 'Indietro', tornate di nuovo alla finestra principale.

8.4.2 Opzioni per la configurazione del boot loader

Per gli utenti meno esperti, la configurazione eseguita con YaST è più semplice che modificare direttamente i file di configurazione. Con il mouse, evidenziate un'opzione e cliccate poi su 'Modifica'. Appare una finestra di dialogo nel quale potete eseguire delle impostazioni individuali. Cliccando su 'OK' confermate le modifiche. Il programma vi riporta alla finestra di dialogo principale, dove potrete modificare altre opzioni. Queste ultime cambiano a seconda del boot loader. GRUB dispone di una serie di opzioni, tra cui:

Tipo di boot loader Questa opzione vi permette di passare da GRUB a LILO e viceversa. Essa vi porta ad un altra finestra di dialogo che serve ad impostare il passaggio. Potete convertire una configurazione GRUB in una configurazione LILO simile. In questo caso, tuttavia, potrebbero andar perse delle informazioni se non vi sono opzioni equivalenti. Potete anche creare una configurazione completamente nuova o farvene proporre una per poi adattarla alle vostre esigenze.

Quando invocate il modulo di configurazione del boot loader con il sistema in esecuzione, potete caricare la configurazione dal disco rigido. Questa opzione vi permetterebbe all'occorrenza di tornare al vecchio boot loader. Questa possibilità sussiste finché non uscite dal modulo del boot loader.

Locazione del boot loader In questa finestra stabilite dove installare il boot loader: nel Master Boot Record (MBR), nel settore di caricamento della partizione boot (se disponibile), nel settore di caricamento della partizione root o su dischetto. Tramite l'opzione 'Altro', potete scegliere un'altra destinazione per l'installazione del boot loader.

Sequenza dei dischi rigidi Se il vostro computer possiede più di un disco rigido, indicate qui la sequenza in base alle impostazioni del BIOS del sistema.

Sezione predefinita Questa opzione serve a determinare il kernel o il sistema operativo da caricare una volta scaduto il tempo massimo di attesa per la selezione da parte dell'utente. In questo menu tramite il pulsante 'Modifica' giungete all'elenco delle voci riportate nel menu di caricamento. Selezionate la voce e cliccate sul pulsante 'Imposta come predefinita'. Per modificare una delle voci, cliccate invece su 'Modifica'.

Sezioni disponibili La finestra principale contiene tutte le voci disponibili nel menu di boot. Selezionando questa opzione e cliccando su 'Modifica', arrivate alla stessa finestra di dialogo di 'Sezione predefinita'.

Abilitare la partizione del boot loader
Con questa opzione, abilitate la partizione nel cui settore di caricamento è stato installato il boot loader, a prescindere dalla partizione sulla quale risiede la directory `/boot` o `/` (root) con i file del boot loader.

Sostituire il codice nell'MBR Se avete installato in precedenza GRUB direttamente nell'MBR o su un disco rigido nuovo di zecca e ora non volete piu installare GRUB nell'MBR, ripristinate tramite questa opzione il codice di boot generico nell'MBR.

Salvare file e settori del disco rigido Le aree modificate del disco rigido vengono salvate.

Aggiungi MBR memorizzato nel menu del boot loader
Aggiunge l'MBR salvato al menu del boot loader.

Un'ultima opzione interessante è anche il 'Timeout', che serve a impostare per quanti secondi il boot loader debba aspettare che venga fatta una selezione da parte dell'utente, prima di caricare il sistema di default. Con il pulsante 'Aggiungi', potete anche impostare altre opzioni. Consultate le rispettive pagine di manuale (`man grub`, `man lilo`). La documentazione è disponbinile (on-line) all'indirizzo: `http://www.gnu.org/software/grub/manual`.

8.5 Rimuovere il bootloader Linux

YaST vi assiste nella disinstallazione del boot loader Linux e nel ripristinare l'MBR allo stato antecedente all'installazione di Linux. Durante l'installazione YaST

crea automaticamente una copia di sicurezza dell' MBR originario e su richiesta lo reinstalla, in modo da sovrascrivere GRUB.

Per disinstallare GRUB avviate il modulo bootloader di YaST ('Sistema' → 'Configurazione del bootloader'). Nella prima finestra selezionate 'Reset' → 'Ripristina MBR dal disco rigido' e uscite dalla finestra con 'Fine'. Nell'MBR a questo punto GRUB viene sovrascritto con i dati dell'MBR originario.

8.6 Creare il CD di avvio

Se doveste incontrare delle difficoltà ad eseguire il boot del vostro sistema o il bootmanager non si lascia installare né nell' MBR del vostro disco rigido né su dischetto, sussiste la possibilità di creare un CD avviabile con tutti file di avvio per Linux richiesti. Chiaramente il vostro sistema dovrà disporre di un masterizzatore di CD.

Per creare un CD-Rom avviabile con GRUB occorre un *stage2* particolare denominato `stage2_eltorito` e facoltativamente e quindi non necessariamente un `menu.lst` su misura. Non sono richiesti i classici file `stage1` e `stage2`.

Create una directory in cui generare l'immagine ISO, per esempio con `cd /tmp` e `mkdir iso`. Create una sottodirectory per GRUB con `mkdir -p iso/boot/grub`. Copiate il file `stage2_eltorito` nella directory `grub`:

```
cp /usr/lib/grub/stage2_eltorito iso/boot/grub
```

Copiate anche il kernel (`/boot/vmlinuz`), `initrd` (`/boot/initrd`) e `/boot/message` sotto `iso/boot/`:

```
cp /boot/message iso/boot/
cp /boot/vmlinuz iso/boot/
cp /boot/initrd iso/boot/
```

Affinché GRUB possa individuare questi file, copiate `menu.lst` sotto `iso/boot/grub` e modificate l'indicazione del percorso in modo che vengono letti i file sul CD sostituendo nell'indicazione del percorso il nome di dispositivo del disco rigido (ad es. `(hd*)`) con il nome di dispositivo del lettore di CD (`(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
```

Create quindi un immagine ISO9660 servendovi del comando riportato di seguito:

```
mkisofs -R -b boot/grub/stage2_eltorito -no-emul-boot \
-boot-load-size 4 -boot-info-table -o grub.iso iso
```

Infine masterizzate il file `grub.iso` risultante su un CD servendovi di un'applicazione di vostra preferenza.

8.7 La schermata grafica SUSE

A partire da SUSE LINUX 7.2, la schermata grafica di SUSE viene visualizzata sulla prima console se utilizzate l'opzione "vga=<value>" quale parametro per il kernel. Se eseguite l'installazione tramite YaST, questa opzione viene abilitata in modo automatico in base alla risoluzione scelta e la scheda grafica. Vi sono tre modi per disabilitare la schermata SUSE:

Disabilitare la schermata SUSE all'occorrenza.
Immettete il comando `echo 0 >/proc/splash` sulla linea di comando per disabilitare la schermata grafica. Per abilitarla nuovamente, immettete `echo 1 >/proc/splash`.

Disabilitare la schermata di SUSE di default.
Aggiungete il parametro del kernel `splash=0` alla configurazione del boot loader. Per maggiori informazioni a riguardo consultate capitolo 8 a pagina 177. Se preferite il modo testo, il default nelle prime versione di SUSE LINUX, impostate `vga=normal`.

Disabilitare completamente la schermata SUSE.
Compilate un nuovo kernel e disabilitate l'opzione 'Use splash screen instead of boot logo' in 'framebuffer support'.

Suggerimento

Se disabilitate il framebuffer support nel kernel disabilitate automaticamente anche lo splash screen. SUSE non potrà elargire del supporto se utilizzate un kernel autocompilato.

Suggerimento

8.8 Difficoltà possibili e la loro risoluzione

In questa sezione vengono illustrate alcune delle eventuali difficoltà che si verificano al boot di . I rimedi possibili verranno presentati brevemente. Alcune tematiche vengono trattate anche in un articolo della banca dati di supporto (`http://portal.suse.de/sdb/en/index.html`). Se il vostro problema in particolare non viene trattato, consigliamo di eseguire una ricerca di articoli che contengono la parola chiave *GRUB*, *boot* e/o *boot loader* servendovi della maschera di ricerca della banca dati di supporto `https://portal.suse.com/PM/page/search.pm`).

GRUB e XFS XFS non lascia nel blocco di boot della partizione alcun spazio per `stage1`. Quindi non potete indicare in alcun caso una partizione con XFS quale locazione del bootloader. In questi casi si consiglia di creare una partizione di boot a sé stante non formatata con XFS.

GRUB e JFS Anche se da un punto di vista meramente tecnico possibile, non si consiglia di combinare GRUB con JFS. In questi casi create una partizione di boot a sé stante `/boot` e formattatela con Ext2. Su questa partizione installate quindi GRUB.

GRUB indica un GRUB Geom Error In fase di avvio GRUB controlla la geometria dei dischi connessi. A volte il BIOS emette delle indicazioni non consistenti in modo che GRUB comunichi un GRUB Geom Error. In questi casi utilizzate LILO o aggiornate eventualmente il BIOS. Informazioni dettagliate riguardanti l'installazione, la configurazione e la manutenzione di LILO sono reperibili nella banca dati di supporto di SUSE, eseguite una ricerca degli articoli di riferimento indicando quale parola chiave della vostra ricerca il lemma LILO.

GRUB emette questo avviso di errore anche in quei casi in cui Linux sia stato installato su un disco rigido aggiuntivo nel sistema, senza che il disco in questione sia stato registrato nel BIOS. La prima parte del bootloader

(*stage1*) viene rilevato e caricato correttamente, ma non viene rilevato il secondo livello (*stage2*). In questi casi si consiglia di registrare il nuovo disco rigido immediatamente nel BIOS.

Sistema IDE-SCSI misto non si avvia

Può verificarsi il caso che rilevi in modo errato la sequenza di boot dei dischi rigidi (e voi non la corregete). Ad esempio, GRUB rileva `/dev/hda` come `hd0` e `/dev/sda` come `hd1` mentre nel BIOS è impostata la sequenza inversa (SCSI *prima* di IDE).

Apportate le correzioni del caso ricorrendo alla riga di comando GRUB; dopo il boot modificate a sistema caricato il file `device.map` per rendere permanete la nuova sequenza. In seguito verificate anche i nomi di dispositivo nei file `/boot/grub/menu.lst` e `/boot/grub/device.map` e reinstallate il bootloader con il seguente comando:

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

Avviare Windows dal secondo disco rigido

Alcuni sistemi operativi (ad es. Windows) possono essere caricati solo dal primo disco rigido. Se un sistema operativo del genere non risiede sul primo disco rigido, nella rispettiva registrazione di menu potete eseguire la seguente modifica:

```
...
title windows
   map (hd0) (hd1)
   map (hd1) (hd0)
   chainloader(hd1,0)+1
...
```

Nell'esempio riportato sopra, Windows deve essere avviato dal secondo disco rigido, a tal fine si modifica la sequenza logica dei dischi con `map`. Tenete comunque presente che con questo cambio *non* si modifica la logica all'interno del file menu di GRUB. Quindi dovete indicare il secondo disco per quel che riguarda `chainloader`.

8.9 Ulteriori informazioni

Sul sito web: `http://www.gnu.org/software/grub/` trovate informazioni dettagliate su GRUB anche in inglese o se preferite in tedesco. Il manuale in

linea è comunque in inglese. Se avete installato texinfo immettendo nella shell `infogrub` visualizzate le pagine info su GRUB. Nella banca dati di supporto potete eseguire una ricerca di articoli attinenti, immettendo “GRUB” quale parola chiave; la banca dati la trovate all’indirizzo `http://portal.suse.de/sdb/en/index.html`.

Il kernel Linux

Il kernel è il cuore di un sistema Linux. Nelle pagine seguenti, non vi mostreremo come diventare kernel "hacker", ma vi indicheremo almeno come eseguire un aggiornamento del kernel e vi metteremo in grado di compilare ed installare un kernel da voi configurato. Se procedete come descritto in questo capitolo, potrete continuare a lavorare con il kernel che avete utilizzato finora avendo la possibilità di caricarlo nuovamente in qualsiasi momento.

Il kernel, che durante l'installazione viene scritto nella directory `/boot`, è configurato in modo tale da supportare un largo spettro di hardware: perciò *non è necessario*, compilare un proprio kernel, almeno ché non vogliate testare feature e driver in fase "sperimentale".

Spesso si può intervenire sul comportamento del kernel tramite cosiddetti parametri del kernel. Ad esempio il parametro `desktop` riduce le fette di tempo (time slice) dello schedulatore in modo che il sistema dà l'impressione di essere più veloce. Per maggiori informazioni rimandiamo alla documentazione sul kernel contenuta nella directory `/usr/src/linux/Documentation`, se avete installato il pacchetto `kernel-source`.

Per creare un nuovo kernel, vi sono dei `Makefiles`, grazie ai quali il processo si svolge in modo quasi del tutto automatico. Solo le domande sull'hardware che il kernel deve supportare devono venire percorse; in maniera interattiva. Dovete conoscere il vostro computer molto bene per fare le scelte giuste, per questo consigliamo – almeno per i primi tentativi – di modificare un file di configurazione già esistente e funzionante per ridurre il rischio di impostazioni errate.

9.1 Aggiornamento del kernel

Per installare un kernel di aggiornamento SUSE scaricate il pacchetto di aggiornamento dal server ftp di YaST o da un mirror come ad esempio: `ftp://ftp.gwdg.de/pub/linux/suse/`. Se non sapete quale Kernel utilizzate attualmente dal vostro sistema, potete farvi mostrare la stringa indicante la versione con `cat /proc/version`. Per maggiori informazioni su YOU (YaST online update) rimandiamo a sezione 2.2.3 a pagina 49.

Durante un update, vi è un finestra popup che spiega come procedere. Seguite i comandi per avere e mantenere un sistema consistente.

9.2 Le sorgenti del kernel

Per poter compilare un kernel è naturalmente necessario che siano installati i sorgenti del kernel (il pacchetto `kernel-source`). Altri pacchetti richiesti come il compiler C (il pacchetto `gcc`), i binutils GNU (il pacchetto `binutils`) ed i file include per il compiler C (`glibc-devel`) vengono selezionati in modo automatico da YaST e vanno installati.

I sorgenti del kernel si trovano ad installazione avvenuta nella directory `/usr/src/linux-<versionedelkernel>`. Se avete in mente di fare qualche esperimento con il kernel e volete disporre contemporaneamente di diverse versioni, conviene scompattare ogni versione in diverse sottodirectory e indirizzare tramite un link i sorgenti rilevanti del momento, dato che vi sono pacchetti software che si aspettono i sorgenti del kernel nella directory `/usr/src/linux`. Questo tipo d'installazione viene eseguita automaticamente da YaST.

9.3 Configurazione del kernel

La configurazione del kernel attualmente in esecuzione la trovate nel file `/proc/config.gz`. Se intendete modificare la configurazione del kernel, andate come `root` nella directory `/usr/src/linux` ed eseguite i comandi:

```
zcat /proc/config.gz > .config
make oldconfig
```

Il comando `make oldconfig` utilizza il file `/usr/src/linux/.config` come template per l'attuale configurazione del kernel. Se ai vostri sorgenti del kernel sono state aggiunte delle opzioni, vi verranno chieste adesso. Se manca il file `.config`, allora si utilizza una configurazione di "default" contenuta nei sorgenti del kernel.

Le opzioni di configurazione del kernel non possono essere trattati in questa sede in modo dettagliato. Potete comunque documentarvi servendovi dei numerosi testi esplicativi sulla configurazione del kernel. La documentazione aggiornata sul kernel è reperibile in `/usr/src/linux/Documentation`.

9.3.1 Configurazione dalla linea di comando

Per configurare il kernel, andate su `/usr/src/linux` e digitate il seguente comando `make config`. Vi verrà chiesto quali funzionalità di sistema debba supportare il kernel. A queste domande di solito potete rispondere in due o tre modi: con un semplice (y) e (n), o con una delle tre possibilità (y) (yes), (n) (no) e (m) (module). (m) qui significa che il driver non è ancora parte integrante del kernel, ma è compilato come modulo che può essere aggiunto al kernel in esecuzione. Naturalmente dovete integrare nel kernel tutti i driver necessari al caricamento del sistema. In questi casi, scegliete perciò (y). Con (Invio) confermate la preselezione che viene letta dal file `.config`. Se ad una domanda premete un tasto diverso, riceverete un breve testo di aiuto riguardante la relativa opzione.

9.3.2 Configurazione nel modo di testo

Per una configurazione più comoda, usate “menuconfig”; eventualmente dovete installare `ncurses-devel` con YaST. Inizializzate la configurazione del kernel con il comando `make menuconfig`.

Non dovrete ripetere la procedura per intero se volete apportare solo delle piccole modifiche alla configurazione, basta selezionare direttamente, tramite il menu, un determinato settore. Le preimpostazioni si trovano in `.config`. Per caricare un’altra configurazione, selezionate la voce del menu ‘Load an Alternate Configuration File’ ed indicate il nome del file.

9.3.3 Configurazione sotto il sistema X Window

Se avete installato il sistema X Window (il pacchetto `xorg-x11`) ed i pacchetti devel di QT (`qt3-devel`, potete, in alternativa, eseguire la configurazione con `make xconfig`. Disporrete di una interfaccia grafica che renderà il processo di configurazione più comodo. A tal fine dovrete lanciare il sistema X Window come utente `root`, immettete il comando `su` per ottenere una `root`-shell con accesso al display. I valori predefiniti vengono letti dal file `.config`. Tenete presente che la configurazione tramite `make xconfig` non è così ben manutenuta come le altre possibilità di configurazione. Quindi dopo questo metodo di configurazione eseguite un `make oldconfig`.

9.4 Moduli del kernel

Vi sono innumerevoli componenti di hardware per PC. Per poter utilizzare correttamente questo hardware, serve un “driver”, tramite il quale il sistema operativo (in Linux il “kernel”) possa indirizzare in modo corretto l’hardware. In linea di massima vi sono due meccanismi per integrare dei driver nel kernel:

- I driver possono essere parte integrante del kernel. Questi kernel “tutti di un pezzo” in questo manuale li chiameremo kernel *monolitici*. Alcuni driver possono essere utilizzati solo in questa variante.
- I driver si possono aggiungere al kernel anche all’occorrenza, in questo caso si parla di kernel *modulare*. Il vantaggio è che vengono caricati solo i driver prettamente necessari senza appesantire inutilmente il kernel.

Al momento della configurazione del kernel si stabilisce quali driver vanno integrati nel kernel e quali assumeranno la forma di moduli. Tutte le componenti del kernel non strettamente necessari al boot, dovrebbero assumere la forma di modulo. In tal modo viene assicurato che il kernel non assume una dimensione gigantesca e che possa venire caricato senza difficoltà dal BIOS e da un boot loader qualsiasi. Il driver del disco rigido, il supporto di `ext2` e driver simili vanno compilate direttamente nel kernel, mentre il supporto per `isofs`, `msdos` o `sound` dovrebbe essere compilato sotto forma di modulo.

Suggerimento

Anche i driver richiesti al boot del system dovrebbero essere integrati sotto forma di moduli. In tal caso l'initial ramdisk carica questi moduli al boot.

Suggerimento

I moduli del kernel si trovano in `/lib/modules/<versione>`. `versione` sta per la versione attuale del kernel.

9.4.1 Rilevamento dell'hardware attuale con hwinfo

hwinfo rileva l'hardware del sistema e seleziona i driver richiesti per eseguire il vostro hardware. Per capire un pò come funziona il programma immettete il comando: `hwinfo --help`. Per ottenere ad esempio i dati sui dispositivi SCSI integrati immettete il comando: `hwinfo --scsi`. Le stesse informazioni le potete ricavare anche tramite YaST nel modulo sulle informazioni hardware.

9.4.2 Utilizzo dei moduli

Per integrare i moduli nel kernel vi è il pacchetto `module-init-tools` che mette a disposizione i seguenti comandi:

`insmod` Con il comando `insmod`, viene caricato il modulo indicato. Il modulo viene cercato in una sottodirectory di `/lib/modules/<versione>`. `insmod` *non* dovrebbe venir più preferito (vd. sotto) a `modprobe`, perché `modprobe` esegue anche una verifica delle dipendenza relative al module.

`rmmod` Elimina il modulo indicato. Ciò è naturalmente consigliabile solo se la corrispondente funzione del kernel non viene più usata. Non è però per esempio, possibile eliminare il modulo `isofs` se un CD è ancora montato.

depmod Questo comando crea un file di nome `modules.dep` nella directory `/lib/modules/<versione>`; nel file sono annotate le dipendenze dei singoli moduli: con ciò si assicura che al momento di caricare un modulo vengano automaticamente caricati anche tutti i moduli dipendenti. Il file con le dipendenze dei moduli viene generato automaticamente all'avvio del sistema, qualora non esistesse già.

modprobe Caricare o scaricare un modulo tenendo conto delle dipendenze dagli altri moduli. Questo comando è molto utile e può venire impiegato anche per altri scopi (p.es. provare tutti i moduli di un determinato tipo finché se ne trovi uno che venga caricato correttamente). Al contrario del caricamento con insmod, modprobe analizza il file `/etc/modprobe.conf` e dovrebbe perciò venire usato per il caricamento dei moduli. Per una spiegazione dettagliata di tutte le opzioni, leggete le corrispondenti pagine di manuale.

lsmod Indica i moduli attualmente caricati e che vengono utilizzati da altri moduli. I moduli caricati dal demone del kernel sono contrassegnati da `autoclean`; ciò significa che questi moduli vengono automaticamente rimossi se non vengono usati per un certo periodo di tempo.

modinfo Vi mostra i dettagli di un modulo. Visto che queste informazioni vengono estratte dal modulo stesso, possono essere visualizzate solo le informazioni incluse dagli sviluppatori di driver. Tra le informazioni che ottenete vi è l'autore, una descrizione, la licenza, parametri del modulo, dipendenze e gli alias.

9.4.3 Il file /etc/modules.conf

Il caricamento dei moduli dipende inoltre dai file `/etc/modules.conf` `/etc/modprobe.conf.local` e la directory `/etc/modprobe.d`; cfr. la pagina di manuale con `man modprobe.conf`. In questo file, possono venire impostati e attivati i parametri per quei moduli che accedono direttamente all'hardware e che devono perciò essere configurati in base al sistema specifico (p.es. driver per il lettore di CD-Rom o driver di rete). I parametri qui registrati vengono descritti nei sorgenti del kernel. Installate il pacchetto `kernel-source` e leggete la relativa documentazione che trovate nella directory `/usr/src/linux/Documentation`.

9.4.4 Kmod – il Kernel Module Loader

La via più elegante di utilizzare i moduli del kernel è senza dubbio quella di ricorrere al "Kernel Module Loader". Kmod lavora in sottofondo e fa sì che vengano caricati automaticamente i moduli necessari, tramite modprobe, non appena si accede alla relativa funzionalità del kernel.

Per poter usare Kmod, dovete abilitare, durante la configurazione del kernel, l'opzione 'Kernel module loader' (`CONFIG_KMOD`). Kmod non è stato ideato per scaricare automaticamente dei moduli; con la quantità di RAM dei computer odierni, il guadagno in termini di RAM sarebbe trascurabile.

9.5 Compilare il kernel

► **x86, AMD64, EM64T**
Noi consigliamo di generare un "bzImage". In questo modo, è generalmente possibile evitare che il kernel diventi "troppo grande"; il che può facilmente verificarsi se si selezionano troppe proprietà e si crea uno "zImage" (le comunicazioni tipiche in questo caso sono kernel too big o System is too big). ◄

Dopo aver configurato il kernel secondo le vostre esigenze, iniziate la compilazione (in `/usr/src/linux/`):

```
make clean
make bzImage
```

Potete inserire entrambi i comandi anche in una linea di comando:

```
make clean bzImage
```

Alla fine della compilazione, troverete il kernel compresso nella directory `/usr/src/linux/arch/<arch>/boot` L'immagine del kernel (il file contenente il kernel) si chiama `bzImage`.

Se non trovate questo file, si è probabilmente verificato un errore durante la compilazione del kernel. Nella bash con

```
make bzImage V=1 2>&1 | tee kernel.out
```

potete rilanciare il processo di compilazione e "protocollarlo" nel file `kernel.out`.

Se avete configurato parti del kernel come moduli caricabili, dovete inizializzare la compilazione di questi moduli. Potete farlo con `make modules`.

9.6 Installare il kernel

Il kernel a questo punto va installato nella directory `/boot` tramite il comando:

```
INSTALL_PATH=/boot make install
```

Installate i moduli compilati; tramite il comando `makemodules_install` potete copiarli nelle directory target corrette sotto `/lib/modules/<versione>`.
In questo caso, i vecchi moduli (con la stessa versione del kernel) vengono sovrascritti; Niente paura! Dai CD potrete ripristinare i moduli originari ed il kernel.

Suggerimento

Assicuratevi di eliminare da `/lib/modules/<versione>` i moduli, le cui funzioni sono state integrate nel kernel, per evitare conseguenze imprevedibili. Per questo motivo, sconsigliamo *vivamente* alle persone inesperte di compilarsi un kernel da sé.

Suggerimento

Affinché GRUB sia in grado di caricare il vecchio kernel (adesso `/boot/vmlinuz.old`) inserite nel file `/boot/grub/menu.lst` anche l'etichetta `Linux.old` come immagine di boot. Questo procedimento viene spiegato in modo dettagliato nel capitolo 8 a pagina 177. Con GRUB non dovete eseguire una reinstallazione.

Da tenere inoltre presente: il file `/boot/System.map` contiene i simboli del kernel necessari ai moduli del kernel per potere richiamare correttamente le funzioni del kernel. Questo file dipende dal kernel attuale; perciò, dopo la compilazione e l'installazione del kernel, si deve copiare il file `/usr/src/linux/System.map` attuale nella directory `/boot`. Questo file viene ricreato ad ogni compilazione del kernel. Se in fase di boot doveste ricevere una comunicazione di errore del tipo System.map does not match actual kernel, vuol dire che probabilmente, dopo la compilazione del kernel, il file `System.map` non è stato copiato sotto `/boot`.

9.7 Pulire il disco rigido dopo la compilazione del kernel

Se sorgono dei problemi dovuti alla mancanza di spazio sul disco, potete cancellare i file oggetto (object file) creati durante la compilazione del kernel eseguendo

`make clean` nella directory `/usr/src/linux`. Se avete però spazio a sufficienza sul disco, e avete intenzione di riconfigurare spesso il kernel, saltate quest'ultimo punto. Quando ricompilerete il kernel, durerà di meno, poiché vengono ricompilate solo quelle parti del sistema soggette a modifiche.

Caratteristiche speciali di SUSE LINUX

Questo capitolo contiene delle indicazioni sui singoli pacchetti software nonché sulle console virtuali e mappatura della tastiera. Il capitolo si chiude con una sezione dedicata alle impostazioni della lingua (I18N/L10N).

10.1 Informazioni su particolari pacchetti di software

10.1.1 Il pacchetto bash ed /etc/profile

Quando invocate una shell di login, la bash processa i file di inizializzazione in questa sequenza:

1. `/etc/profile`
2. `~/.profile`
3. `/etc/bash.bashrc`
4. `~/.bashrc`

Gli utenti possono eseguire registrazioni proprie in `~/.profile` o `~/.bashrc`. Per garantire un'elaborazione corretta dei file è necessario che si assumono le impostazioni basilari di `/etc/skel/.profile` o `/etc/skel/.bashrc` nella directory home dell'utente. Dopo un update si consiglia di orientarsi alle impostazioni di `/etc/skel`; per non perdere propri adattamenti eseguiti questo comando:

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

In seguito dovete ricopiare i vostri adattamenti dal file `*.old`.

10.1.2 Il pacchetto cron

Le tabelle `cron` si trovano sotto `/var/spool/cron/tabs`. `/etc/crontab` funge da tabella cron valida per tutto il sistema. Indicate direttamente dopo l'indicazione dell'ora l'utente che debba eseguire il comando (cfr. l'esempio 10.1 nella pagina successiva, che indica `root`); i dati dei pacchetti in `/etc/cron.d` hanno lo stesso formato, si veda `man cron`.

Esempio 10.1: *Esempio di una registrazione in /etc/crontab*

```
1-59/5 * * * * root test -x /usr/sbin/atrun && /usr/sbin/atrun
```

`/etc/crontab` *non* può essere modificato con `crontab -e`, ma deve venire direttamente caricato in un editor, modificato ed infine salvato.

Alcuni pacchetti installano, nelle directory `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` e `/etc/cron.monthly` degli script di shell, la cui elaborazione viene diretta da `/usr/lib/cron/run-crons` che viene invocato ogni 15 minuti dalla tabella principale (`/etc/contrab`); in questo modo, si assicura che vengano recuperate per tempo esecuzioni mancate.

Per motivi di chiarezza sono diversi script che si occupano della manutenzione quotidiana; questi script sono contenuti nel pacchetto `aaa_base`. In `/etc/cron.daily` vi è p.es. `backup-rpmdb`, `clean-tmp` o `clean-vi`.

10.1.3 File di log — il pacchetto logrotate

Molti servizi di sistema (ingl. daemon) ed il kernel stesso protocollano regolarmente lo stato del sistema od eventi particolari nei cosiddetti file protocollo (ingl. log files) che l'amministratore può consultare in qualsiasi momento per determinare lo stato del sistema in un momento particolare, nonché ricercare ed ovviare ad errori o malfunzionamenti. Come previsto dall'FHS, questi log file vengono normalmente memorizzati nella directory `/var/log`, il cui contenuto cresce di giorno in giorno. Con l'aiuto di `logrotate`, potete tenere sotto controllo il volume dei file di protocollo.

Configurazione

Nel file di configurazione `/etc/logrotate.conf`, viene determinato il comportamento generale. Con `include`, in particolare, si imposta quali altri file debbano essere analizzati; su è previsto che i singoli pacchetti di `/etc/logrotate.d` installino dei file (ad esempio, `syslog` o `yast`).

Esempio 10.2: *Esempio di /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, invece, viene controllato tramite cron ed avviato da `/etc/cron.daily/logrotate` una volta al giorno.

Importante

L'opzione `create` carica in memoria le impostazioni dei file `/etc/permissions*` eseguite dall'amministratore. Assicuratevi sempre che le vostre modifiche non creino dei conflitti.

Importante

10.1.4 Pagine di manuale

Per alcuni programmi GNU (per esempio tar), le pagine di manuale non vengono più aggiornate. Al loro posto, troverete un sommario nell'output di `--help` e un manuale dettagliato nei file Info. Info è il sistema ipertestuale di GNU. Con `info info` otterrete delle prime istruzioni per l'uso. Potete utilizzare Emacs per accedere alle pagine `info`, immettete `emacs -f info` o semplicemente con il comando `info` in una console. Comodi da utilizzare sono tkinfo, xinfo; o il sistema di aiuto SUSE per la visualizzazione delle pagine info.

10.1.5 Il comando locate

locate, che permette di trovare velocemente dei file, non fa parte della gamma software installata di default. Potete installarlo successivamente (`find-locate`). Il processo updatedb viene avviato automaticamente ogni notte o ca. 15 minuti dopo il boot del sistema.

10.1.6 Il comando ulimit

Con il comando `ulimit` (ingl. *user limits*), potrete limitare l'uso delle risorse di sistema o visualizzarle. `ulimit` è particolarmente adatto a limitare la memoria disponibile alle applicazioni. In questo modo, si può impedire che un'applicazione occupi troppo (o tutto lo) spazio di memoria, causando così il blocco del sistema.

Potrete lanciare di `ulimit` con opzioni diverse. Per limitare l'uso di memoria, usate le opzioni riportate nella tabella 10.1 in questa pagina.

Tabella 10.1: *ulimit: impostare le risorse dell'utente*

`-m`	grandezza massima della memoria fisica
`-v`	grandezza massima della memoria virtuale
`-s`	grandezza massima dello stack
`-c`	grandezza massima dei core file
`-a`	visualizzazione dei limiti impostati.

Le impostazioni valide per l'intero sistema possono venire effettuate in `/etc/profile`. Una delle impostazioni consiste nell'autorizzare la creazione di quei core file necessari ai programmatori per il *debug*. L'utente normale non ha il permesso di aumentare i valori impostati dall'amministratore del sistema in `/etc/profile`; può però inserire determinate impostazioni nel proprio `~/.bashrc`.

Esempio 10.3: *Impostazioni ulimit in /.bashrc*

```
# Limite della memoria fisica:
ulimit -m 98304

# Limite della memoria virtuale:
ulimit -v 98304
```

La memoria viene espressa in Kbyte. Per informazioni più dettagliate, consultate `man bash`.

Importante

Non tutte le shell supportano le direttive `ulimit`. Se non potete fare a meno di questo tipo di restrizioni, PAM (p.es. `pam_limits`) offre ampie possibilità di impostazione.

Importante

10.1.7 Il comando free

Il nome del comando `free` è un pò fuorviante, dal momento che questo comando serve a verificare quanta memoria venga attualmente utilizzata . . . . Troverete le informazioni essenziali in `/proc/meminfo`. Al giorno d'oggi, l'utente di un sistema moderno come Linux non dovrebbe preoccuparsene più di tanto. Il concetto di "RAM disponibile" risale ai tempi quando non vi erano ancora sistemi di gestione unitaria della memoria (ingl. unified memory management). Il motto di Linux è: *la memoria libera è cattiva memoria* (ingl. free memory is bad memory), il che vuol dire che Linux cerca sempre di bilanciare le varie cache, senza lasciare della memoria del tutto inutilizzata.

Di per sé, il kernel non sa nulla di applicazioni o dati dell'utente, perché li amministra in cosiddette "Page Cache". Quando la memoria si va esaurendo, parte di questi dati vengono spostati nella partizione swap o nei file dai quali sono stati originariamente estratti con la chiamata di sistema `mmap` (si veda `man mmap`).

Inoltre, il kernel dispone anche di altre cache, come la cosiddetta "slab cache", che contiene anche un buffer usato per l'accesso alla rete. Così si spiegano tutte le differenze tra i contatori di `/proc/meminfo`. La maggior parte delle cache (ma non tutte) possono essere consultate attraverso `/proc/slabinfo`.

10.1.8 Il file /etc/resolv.conf

La risoluzione del nome di dominio viene gestita tramite il file `/etc/resolv.conf`; cfr. il capitolo 24 a pagina 445.

Questo file viene attualizzato solo dallo script `/sbin/modify_resolvconf`. A nessun altro programma è consentito farlo. Solo così si può assicurare che la configurazione della rete ed i relativi dati rimangono consistenti.

10.1.9 Impostazioni per GNU Emacs

GNU Emacs è un ambiente di lavoro complesso; ulteriori informazioni sono reperibili sotto: `http://www.gnu.org/software/emacs/`. Nei seguenti paragrafi indicheremo quali file di configurazione vengono processati da GNU Emacs al suo avvio.

Al suo avvio Emacs legge diversi file che contengono le impostazioni dell'utente, amministratore di sistema e/o distribuzione per poter essere adattato alle specifiche richieste o per poter essere preconfigurato. Nella directory home viene installato per ogni utente il file di inizializzazione `~/.emacs` da `/etc/skel`; `.emacs` a sua volta legge il file `/etc/skel/.gnu-emacs`. Se un utente vorrebbe effettuare degli adattamenti propri, si consiglia di copiare `.gnu-emacs` nella propria directory home (con `cp /etc/skel/.gnu-emacs ~/.gnu-emacs`) e di editarlo lì:

`.gnu-emacs` imposta il file `~/.gnu-emacs-custom` come `custom-file`; se l'utente vuole effettuare delle impostazioni proprie ricorrendo alle possibilità offerte da `customize`, esse saranno memorizzate sotto `~/.gnu-emacs-custom`.

Con SUSE LINUX il pacchetto `emacs` installa il file `site-start.el` nella directory `/usr/share/emacs/site-lisp`. Il file `site-start.el` viene caricato *prima* del file di inizializzazione `~/.emacs`. `site-start.el` garantendo che vengano caricati automaticamente anche file di configurazione speciali distribuiti con i pacchetti aggiuntivi (ingl. add-on) di Emacs (p. es. il pacchetto `psgml`); file di configurazione di questo tipo si trovano anche sotto `/usr/share/emacs/site-lisp` ed iniziano sempre con `suse-start-`. L'amministratore di sistema locale può effettuare nel file `default.el` delle impostazioni che avranno validità per l'intero sistema.

Ulteriori informazioni su questi file solo reperibili nel file info di Emacs, nell' *Init File*: `info:/emacs/InitFile` dove inoltre viene descritto come evitare all'occorrenza che questo file venga caricato.

Le componenti di Emacs sono suddivisi in diversi pacchetti:

- Il pacchetto base `emacs`.
- `emacs-x11` (di solito già installato): il programma *con* supporto per X11.
- Nel pacchetto `emacs-nox` trovate il programma *senza* supporto per X11.
- Il pacchetto `emacs-info` contiene la documentazione in linea nel formato Info.

- Il pacchetto `emacs-el` contiene i file di libreria non compilati in Emacs Lisp; non sono necessari in fase di esecuzione!
- Numerosi pacchetti aggiuntivi che possono essere installati all'occorrenza: il pacchetto `emacs-auctex` (per LaTeX); `psgml` (per SGML/XML); `gnuserv` (per uso client/server) e altri ancora.

10.1.10 vi: una breve introduzione

Ancor oggi si ricorre a degli editor di testo per lavori di ritocco al sistema ma soprattutto per lavori di programmazione. Nel corso degli anni in ambito Unix si è affermato il vi quale editor che si distingue per funzionalità e che da un punto di vista ergonomico eclissa anche degli editor basati su mouse.

Modi operativi:

Fondamentalmente per quanto concerne l'editor "vi" si distinguono tre modi operativi; il modo *insert*, il modo *command* ed il modo *extended*. Nella fase di rodaggio il fatto che i tasti hanno funzioni diverse a secondo del modo abilitato può dare adito a confusione. Illustreremo quindi di seguito metodi comuni per passare da un modo operativo all'altro. Dopo il suo avvio il vi normalmente si trova nel modo *command*.

Modo command → modo insert Esistono numerose via per realizzare questo passaggio, le più comuni sono: (A) per append, (I) per insert oppure (O) per avere un nuovo rigo al di sotto del rigo attuale.

Modo insert → modo command Per uscire dal modo *insert* premete il tasto (ESC). Nel modo *insert* non è possibile terminare il vi. Quindi a tal fine, tenete sempre bene in mente il tasto (ESC).

Modo command → modo extended Il modo *extended* del vi può essere attivato tramite i due punti ((:)). Il modo *extended*, chiamato anche modo *ex* rappresenta in fondo un editor testuale con il quale espletare una serie di operazioni anche di una certa complessità.

Modo extended → modo command Dopo l'esecuzione di un comando nel modo *extended* ci si ritrova nel modo *command*. Se vi trovate nel modo *extended* e non desiderate eseguire alcun comando, potete cancellare i due punti servendovi del tasto (←) e ritornerete nel modo *command*.

Tenete presente che per passare dal modo *insert* al modo *extended* è richiesto sempre un passaggio intermedio per il modo *Command*. Non è quindi possibile eseguire un passaggio diretto.

Agli inizi può causare delle difficoltà uscire da un nuovo editor, il vi qui non rappresenta affatto una eccezione. Cosa da tenere sempre bene in mente è che non potete uscire dal "vi" se vi trovate nel modo *insert*. Dovete prima uscire dal modo *insert* tramite il tasto (ESC), ed in seguito si hanno due casi:

1. *Uscire senza salvare:* se intendete terminare l'editor senza salvare le modifiche, nel modo (:)(Q)(!) fa sì che il "vi" ignora le modifiche apportate.
2. *Uscire e salvare:* per salvare le modifiche apportate e terminare in seguito l'editor potete scegliere tra possibilità diverse. Nel modo *command* vi è il comando (Shift)(Z)(Z). Nel modo *extended* vi è inoltre `:wq` per uscire dal programma. Come avrete già intuito nel modo *extended* si dovrà immettere (:)(W)(Q).

Il vi nell'uso quotidiano

Il vi può essere utilizzato alla stregua di un editor comune. Non appena entrate nel modo *insert* potete immettere del testo e cancellarlo ricorrendo ai tasti (←) e (Canc). Per muovere il cursore potete utilizzare i tasti freccia.

Spesso però vi sono delle difficoltà dovute al fatto che esistono numerosi tipi di terminale con ognuno particolari codice dei tasti (key code). A questo punto entra in gioco il modo *command*. Passate dal modo *insert* a quello *command* premendo il tasto (ESC). Nel modo *command* potete muovere il cursore tramite i tasti (H), (J), (K) e (L). Leggenda:

(H) spostarsi di un carattere verso sinistra

(J) spostarsi di un rigo verso il basso

(K) spostarsi di un rigo verso l'alto

(L) spostarsi di un carattere verso destra

I comandi nel modo *command* di vi possono essere eseguiti in maniera diversa. Di sicuro interesse è la possibilità di ripetere un comando varie volte, basta indicare il numero delle volte il comando debba essere ripetuto e fare seguire il comando vero e proprio. Immettendo quindi (5)(L) il cursore si sposterà verso destra per cinque volte.

Ulteriori informazioni

Il vi offre un vasto numero di comandi. Potete utilizzare delle macro, ricorrere a delle abbreviazioni, a buffer denominati e tante altre cose di sicura utilità. Descrivere tutte queste funzionalità in modo dettagliato ci porterebbe troppo lontano. A questo punto bisogna tuttavia ricordare che SUSE LINUX include una versione ottimizzata del vi ovvero vim (che sta per vi improved). Per chi vuole cimentarsi non mancano le fonti di informazione:

- vimtutor un programma didattico interattivo per vim.
- Se vi serve aiuto, in vim il comando del caso è `:help`
- Su Internet trovate un manuale (in inglese) che tratta vim; l'indirizzo è `http://www.truth.sk/vim/vimbook-OPL.pdf`.
- Per le novità, mailing list e documentazione visitate il sito web del progetto vim che trovate sotto: `http://www.vim.org`.
- Tra i tutorial per vim reperibili su Internet vi sono: `http://www.selflinux.org/selflinux/html/vim.html`, `http://www.linuxgazette.com/node/view/9039` e `http://www.apmaths.uwo.ca/~xli/vim/vim_tutorial.html`. Per ulteriori link riferiti ai tutorial, visitate il sito `http://linux-universe.com/HOWTO/Vim-HOWTO/vim-tutorial.html`.

Importante

La licenza VIM

vim è un cosiddetto "charityware", il che vuol dire che gli autori non vi chiedono dei soldi per il software ma di devolvere una somma a sostegno di un progetto di beneficenza. Nella fattispecie si tratta di un progetto a sostegno dei bambini in Uganda. Per ulteriori dettagli consultate i siti: `http://iccf-holland.org/index.html`, `http://www.vim.org/iccf/` e `http://www.iccf.nl/`.

Importante

10.2 Console virtuali

Linux è un sistema multitasking e multiutente e, anche se avete un sistema per così dire monoutente, imparerete certamente ad apprezzare i vantaggi di queste

funzionalità. Nella modalità testuale sono a vostra disposizione sei console virtuali; premendo la combinazione di tasti (Alt)-(F1) fino a(Alt)-(F6), potete passare da una console all'altra. La settima console è riservata a X11. Modificando il file `/etc/inittab`, potete anche determinare il numero di console disponibili.

Se, da X11, volete ritornare su una console di testo senza però chiudere X11, usate la combinazione (Ctrl)-(Alt)-(F1)fino a (F6). Con (Alt)-(F7) ritornate a X11.

10.3 Mappatura della tastiera

Per uniformare l'impostazione della tastiera nei programmi sono state eseguite delle modifiche ai seguenti file:

```
/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/<VERSIONE>/site-lisp/term/*.el
```

Queste modifiche interessano solo le applicazioni che utilizzano `terminfo`, o i cui file di configurazione sono stati modificati direttamente (`vi`, `less` etc.). Altre applicazioni non- SUSE LINUX devono venire adattate a queste impostazioni di default.

In X il tasto compose (multikey) si ottiene tramite la combinazione di tasti (Ctrl)-(Shift) (destro); cfr. la relativa registrazione in `/usr/X11R6/lib/X11/Xmodmap`.

Sussiste la possibilità di eseguire delle impostazioni mirate tramite l' "X Keyboard Extension" (XKB). Questa estensione viene utilizzata anche negli ambienti desktop GNOME (gswitchit) e KDE (kxkb). Per maggiori informazioni su XKB, rimandiamo a `/etc/X11/xkb/README` e ai documenti lì menzionati.

Per le particolarità in tema di caratteri cinesi, giapponesi e coreani (CJK) consultate il sito allestito da Mike Fabian: `http://www.suse.de/~mfabian/suse-cjk/input.html`.

10.4 Adattamenti nazionali

SUSE LINUX è internazionalizzato e può venire adattato alle condizioni locali; cioé, l'internazionalizzazione (*I18N*) consente localizzazioni speciali (*L10N*). Le abbreviazioni I18N e L10N stanno per internazionalizzazione (*internationalization*) e localizzazione (*localization*) rispettivamente abbreviati con la prima e l'ultima lettera, e in mezzo il numero delle lettere omesse.

Le impostazioni vengono eseguite tramite le variabili `LC_` definite nel file `/etc/sysconfig/language`. Naturalmente non si tratta solo dell'impostazione della lingua dell'interfaccia di una applicazione e comunicazioni dei programmi (ingl. native language support), ma anche delle categorie per *Messaggi* (lingua), *Classe dei caratteri*, *Sequenza della classificazione*, *Data e ora*, *Numeri* e *Valuta*. Ognuna di queste categorie può venire determinata direttamente tramite una propria variabile o indirettamente tramite una variabile superiore nel file `language` (si veda la pagina di manuale `man locale`).:

`RC_LC_MESSAGES`, `RC_LC_CTYPE`, `RC_LC_COLLATE`, `RC_LC_TIME`, `RC_LC_NUMERIC`, `RC_LC_MONETARY`
: Queste variabili vengono consegnate alla shell senza il prefisso `RC_` e determinano le suddette categorie; i file in questione sono elencati qui di seguito. Potete visualizzare le impostazioni attuali tramite il comando `locale`.

`RC_LC_ALL` Questa variabile sovrascrive, se configurata, i valori delle variabili nominate sopra.

`RC_LANG` Questo è il cosiddetto fallback, ossia impostazione di ripiego nel caso nessuna delle suddette variabili sia stata configurata; di default, SUSE LINUX imposta solo `RC_LANG`; in questo modo, l'utente può immettere più facilmente propri valori.

`ROOT_USES_LANG` Si tratta di una variabile `yes/no`. Se è impostata su `no`, `root` lavora sempre nell'ambiente POSIX.

Le variabili vanno impostate tramite l'editor sysconfig di YaST. Il valore di tali variabili è composto dall'indicazione della lingua (ingl. language code), paese o territorio (ingl. country code), set dei caratteri (ingl. encoding) e l'opzione modifier. Le singole indicazioni vengono collegate con caratteri speciali:

```
LANG=<language>[[_<COUNTRY>].<Encoding>[@<Modifier>]]
```

10.4.1 Esempi

Impostate sempre lingua e nazione insieme. L'indicazione della lingua segue lo standard ISO 639 (`http://www.evertype.com/standards/iso639/iso639-en.html` e `http://www.loc.gov/standards/iso639-2/`). I codici dei paesi sono elencati in ISO 3166 (si veda `http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html`). E' consigliabile impostare valori per i quali vi sono dei file di descrizione utilizzabili sotto `/usr/lib/locale`. Ulteriori file di descrizione possono venire creati dai file presi da `/usr/share/i18n` tramite il comando `localedef`; i file descrizione fanno parte del pacchetto `glibc-i18ndata`. Un file di descrizione per `it_IT.UTF-8` viene creato con il comando:

```
localedef -i it_IT -f UTF-8 it_IT.UTF-8
```

`LANG=it_IT.UTF-8` Questa è l'impostazione di default se si esegue l'installazione in italiano; se eseguite l'installazione in un'altra lingua viene impostato anche UTF-8 come set di caratteri, ma viene impostata la rispettiva lingua per il sistema.

`LANG=it_IT.ISO-8859-1` Per la lingua italiana si imposta il set di caratteri `ISO-8859-1` che non contiene il simbolo dell'Euro; questo set di caratteri si usa se un programma non supporta ancora `UTF-8`. L'indicazione del set di caratteri (qui `ISO-8859-1`) viene p.es. utilizzata da applicazioni come Emacs.

`LANG=it_IT@euro` L'esempio riportato sopra include esplicitamente il simbolo dell'Euro nell'impostazione della lingua. Questa indicazione esplicita non è richiesta con UTF-8 perché nclude già il simbolo dell'Euro. Quindi si tratta di una indicazione utile solo se l'applicazione non supporta UTF-8, bensì ISO-8859-15.

SuSEconfig legge le variabili in `/etc/sysconfig/language` e scrive le modifiche necessarie in `/etc/SuSEconfig/profile` e `/etc/SuSEconfig/csh.cshrc`. `/etc/SuSEconfig/profile` viene letto da `/etc/profile` e `/etc/SuSEconfig/csh.cshrc` da `/etc/csh.cshrc`. In questo modo le impostazioni sono disponibili per tutto il sistema.

Gli utenti possono sovrascrivere i valori di default in `~/.bashrc`. Se si imposta `it_IT` e non è si soddisfatti delle comunicazioni del programma in lingua italiana, si può cambiare lingua ed impostare ad esempio la lingua inglese: `LC_MESSAGES=en_US`

10.4.2 Impostazioni per il supporto della lingua

Generalmente, per ottenere una soluzione di ripiego, i file della categoria *Messaggi* vengono archiviati solo nella directory della lingua corrispondente (p.es. `it`). Se quindi `LANG` viene impostato su `it_CH` e se il file *message* non esiste sotto `/usr/share/locale/it_CH/LC_MESSAGES`, si ricorre come ripiego a `/usr/share/locale/it/LC_MESSAGES`.

Con `LANGUAGE` è anche possibile determinare una cascata di fallback; p.es. bretone → francese o il gallego → spagnolo → portoghese:

```
LANGUAGE="br_FR:fr_FR"
```

```
LANGUAGE="gl_ES:es_ES:pt_PT"
```

Oppure potete ricorrere a varianti del norvegese: *nynorsk* e *bokmål* (con ulteriore fallback su `no`):

```
LANG="nn_NO"
```

```
LANGUAGE="nn_NO:nb_NO:no"
```

o

```
LANG="nb_NO"
```

```
LANGUAGE="nb_NO:nn_NO:no"
```

Nel caso del norvegese va tenuto presente che, `LC_TIME` va trattato diversamente.

Il punto decimale in cifre del tipo 1.000 non viene riconosciuto. Probabilmente `LANG` si trova su `it`. Poiché la descrizione alla quale ricorre glibc si trova in `/usr/share/lib/it_IT/LC_NUMERIC`, `LC_NUMERIC` deve venire impostato su `it_IT`.

10.4.3 Ulteriori informazioni:

- *The GNU C Library Reference Manual*, capitolo "Locales and Internationalization"; contenuto nel `glibc-info`.
- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux*, attualmente sotto `http://www.cl.cam.ac.uk/~mgk25/unicode.html`.
- *Unicode-Howto* di Bruno Haible `file:/usr/share/doc/howto/en/html/Unicode-HOWTO.html`.

Il sistema X Window

Sotto Unix il sistema X window (X11) rappresenta de facto lo standard in tema di GUI (interfaccia grafica dell'utente): inoltre X11 è basato sulla rete in modo che l'output di applicazioni che girano su di un computer possono essere visualizzate su di un altro, sempre che i computer siano connessi via rete. La rete può essere una rete LAN, oppure WAN, cioé i computer possono anche comunicare via Internet.

In questo capitolo, vi illustreremo come ottimizzare il vostro ambiente del sistema X window, faremo luce su alcune nozioni fondamentali riguardanti l'utilizzo dei font sotto SUSE LINUX e tratteremo la configurazione di OpenGL/3D.

11.1 Impostazione di X11 tramite SaX2

La superficie grafica, ossia l'X server, gestisce la comunicazione tra hardware e software. I desktop come KDE e GNOME possono pertanto visualizzare informazioni sullo schermo, in modo tale che l'utente possa accedervi. I desktop e tutte le applicazioni simili vengono spesso definite *window manager*. Su Linux ve ne sono molti e possono differenziarsi a volte anche notevolmente nell'aspetto e nelle funzioni.

La superficie grafica viene configurata durante l'installazione. Per modificarne i parametri servitevi di SaX2.

Vengono mostrate le impostazioni attuali e avete modo di resatterle in qualsiasi momento, si tratta della risoluzione dello schermo, profondità cromatica, frequenza di ripetizione, produttore ed il tipo del monitor, se sono stati rilevati automaticamente.

Se avete appena installato il sistema o una nuova scheda grafica, apparirà un'altra piccola finestra, nella quale vi si chiede se attivare l'accelerazione 3D (tridimensionale) per la vostra scheda grafica. Cliccate su 'Modifica': verrà avviato SaX2, lo strumento di configurazione dei dispositivi di immissione e visualizzazione, in una finestra a parte (si veda la figura 11.1 a fronte).

Nella barra di navigazione a sinistra, vedete quattro punti principali: 'Desktop', 'Dispositivi di immissione', 'Multihead' 'Dispositivi di immissione', 'AccessX'. 'Desktop' è la sezione dedicata all'impostazione dello schermo, della scheda grafica, della profondità cromatica, della risoluzione, posizione e dimensione della schermata. Alla voce 'Dispositivi di immissione', potete configurare tastiera e mouse, nonché, schermo tattile ed una tavola grafica. Nel menu 'Multihead', invece, potete impostare un sistema a più schermi (si veda la sezione 11.1.7 a pagina 230). 'AccessX' è uno strumento utilissimo, che serve a muovere il puntatore del mouse con il tastierino numerico.

Selezionate il modello del vostro monitor e la scheda grafica. Se vengono riconosciuti automaticamente dal sistema, non sarà necessaria alcuna modifica. Se il vostro monitor non viene riconosciuto automaticamente, il programma apre una finestra di selezione monitor. Questo dialogo vi offre una lista completa delle case produttrici e modelli. Se non trovate il vostro, immettete i valori indicati dalla documentazione del vostro monitor o selezionate uno dei "modi Vesa" preconfigurati.

A conclusione delle vostre impostazioni riguardanti il monitor e scheda grafica, cliccando su 'Chiudi' nella finestra principale, vi sarà offerta la possibilità di

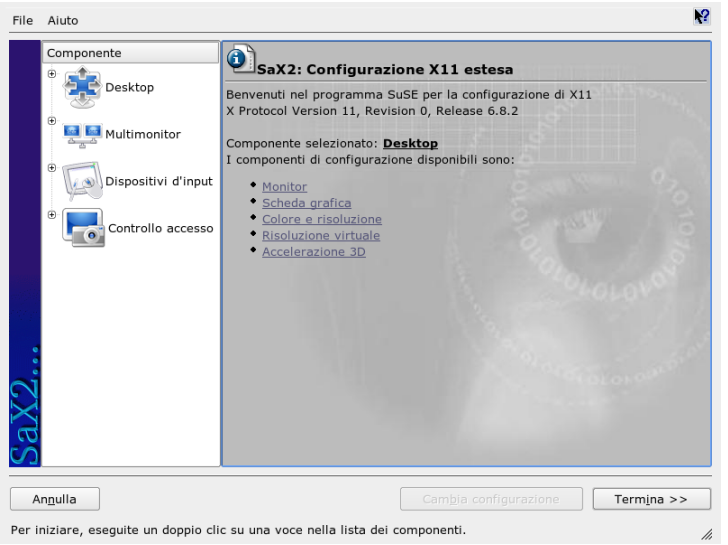

Figura 11.1: *La finestra principale del nuovo SaX2*

testare la vostra configurazione. In questo modo potrete verificare che la configurazione vada bene per i dispositivi. Se, durante il test, l'immagine del monitor dovesse essere disturbata, interrompete il test con il tasto Esc e riducete i valori della frequenza di ripetizione, della definizione o della profondità cromatica. Tutte le vostre modifiche, indipendentemente dal test, verranno applicate dopo aver riavviato il sistema grafico, vale a dire l'X server. Se state usando KDE, basta uscire e rifare il login.

11.1.1 Desktop

Cliccate su 'Modifica configurazione' → 'Proprietà' ed apparirà una finestra con le tre guide 'Monitor', 'Frequenze' ed 'Esteso':

'Monitor' Sulla sinistra della finestra, scegliete il produttore e, a destra, il modello. Se siete in possesso di dischetti con driver Linux per il monitor, potete installarli dopo aver cliccato su 'Dischetto driver'.

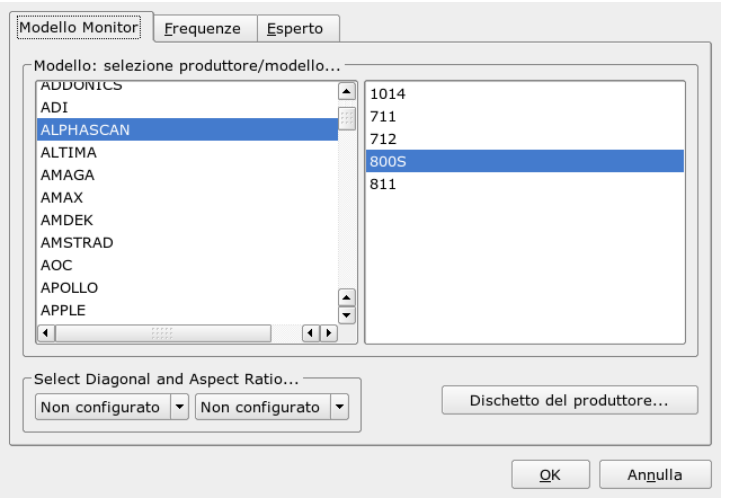

Figura 11.2: *Selezionare il monitor*

'Frequenze' Qui potete configurare le frequenze orizzontali e verticali del vostro schermo. La frequenza verticale non è altro che la frequenza di ripetizione dell'immagine. Normalmente, il programma sonderà i valori massimi e minimi del modello e ve li mostrerà in questo dialogo. Di solito, non sarà necessario apportare delle modifiche.

'Esteso' Impostate qui ancora delle opzioni per il vostro schermo. Nell'area di selezione in alto, potete impostare il metodo di calcolo della definizione e della geometria della schermata. Modificate i valori preimpostati solo se questi sono sbagliati e, nel test, non riuscite ad ottenere un'immagine stabile. Potete anche impostare le dimensioni della videata ed il modo di risparmio energetico DPMS.

Avvertimento

Configurazione delle frequenze del monitor

Siate molto cauti quando configurate le frequenze consentite manualmente, anche se vi sono dei meccanismi di protezione per evitare dei danni. Dei valori errati possono danneggiare seriamente il vostro monitor. Attenetevi ai valori indicati nel manuale del vostro monitor.

Avvertimento

11.1.2 Scheda grafica

Nella finestra della scheda grafica avete due guide: 'Generale' ed 'Per esperti ...'. Sotto 'Generale' selezionate la casa prodruttrice (a sinistra) ed il modello (a destra) della vostra scheda grafica.

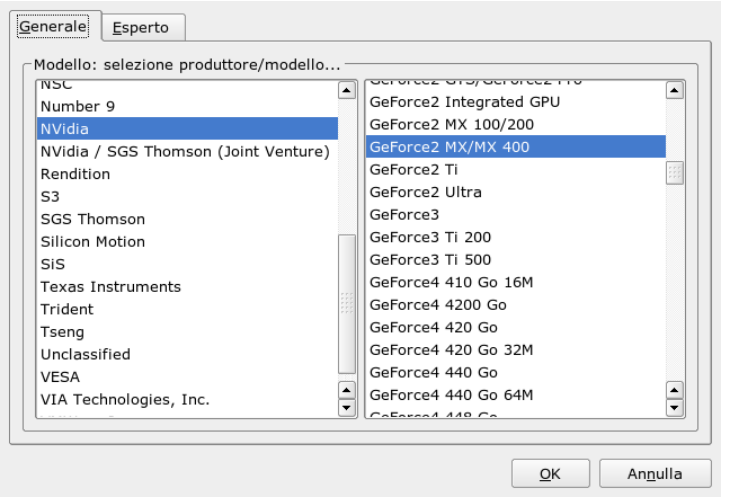

Figura 11.3: *Selezionare la scheda grafica*

'Per esperti ...' offre il modo di intervenire su impostazioni avanzate. A destra determinate se il vostro schermo debba essere ruotato verso sinistra o perpendicolarmente (come nel caso di alcuni schermi TFT). I valori di BusID possono

restare così come sono, dal momento che servono solo con sistemi multischermo. Non modificate neanche le opzioni delle schede, specialmente se non ve ne intendete e non sapete cosa significhino. In caso di necessità, vi preghiamo di leggere attentamente la documentazione della vostra scheda.

11.1.3 Colori/Risoluzione

Anche qui, troverete tre guide: 'Colori', 'Risoluzione' e 'Per esperti ...'.

'Colori' In base al vostro hardware, potete selezionare in tema di profondità di colore tra i valori 16, 256, 32768, 65536 e 16,7 milioni di colori (4, 8, 15, 16 o 24 bit). Per una buona immagine, vi consigliamo di non scegliere meno di 256 colori.

'Risoluzione' Il modulo vi propone tutte le combinazioni di risoluzione e profondità cromatica che possano essere visualizzate dal vostro hardware correttamente. Pertanto, con SUSE LINUX non si corre quasi alcun pericolo di danneggiare l'hardware con impostazioni sbagliate. Se, tuttavia, avete intenzione di cambiare la risoluzione manualmente, vi preghiamo di leggere attentamente la documentazione del vostro hardware e di assicurarvi che i nuovi valori possano essere visualizzati.

'Per esperti...' Qui potete qui aggiungere dei propri valori di risoluzione, i quali verranno poi aggiunti alla selezione generale.

11.1.4 Risoluzione virtuale

Ogni desktop ha propri valori di risoluzione per tutto lo schermo. Accanto a questi valori, se ne possono impostare altri che vanno al di là dello schermo visibile. Ogni volta che valicate i limiti dello schermo con il mouse, l'area virtuale invade quella visibile. Il numero di pixel non cambia, ma aumenta la superficie utile del monitor: questo fenomeno è chiamato "risoluzione virtuale".

Potete impostare la risoluzione virtuale in due modi: uno è 'Tramite Drag&Drop'. Quando il cursore del mouse si trova sull'immagine del monitor, il cursore diventa una crocetta. Tenete premuto il tasto sinistro del mouse e spostate contemporaneamente il mouse incrementando il valore dei reticoli del monitor. Questo valore corrisponde alla risoluzione virtuale. Questo metodo si consiglia soprattutto in quei casi in cui non siete ancora sicuri di quanto spazio virtuale volete disporre sul vostro desktop.

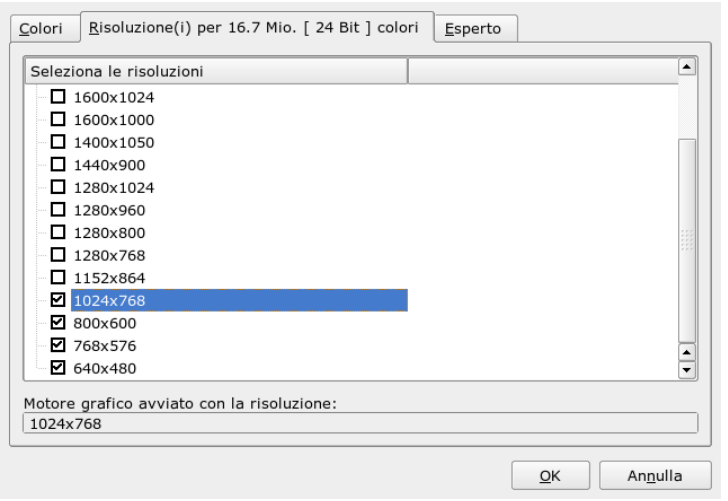

Figura 11.4: *Impostare la risoluzione*

L'altra via è rappresentata da 'Con il menù a popup'. Il menù a popup che si trova al centro della griglia, vi mostra la risoluzione virtuale attualmente impostata. Se sapete già che intendete usare una risoluzione standard come risoluzione virtuale, selezionatela tra quelle proposte dal menù.

11.1.5 Accelerazione 3D

Se, durante la prima installazione o durante l'installazione di una nuova scheda grafica, vi siete dimenticati di abilitare l'accelerazione 3D, potete farlo ora.

11.1.6 Posizione e dimensione dell'immagine

Potete calibrare la posizione e le dimensioni della videata con i tasti-freccia (si veda la figura 11.6 a pagina 231). Se avete un ambiente "multihead" (più di uno schermo), potete passare da un monitor all'altro con il pulsante 'Schermo successivo', per impostare dimensioni e posizione delle schermate. Salvate la configurazione con 'Salva'.

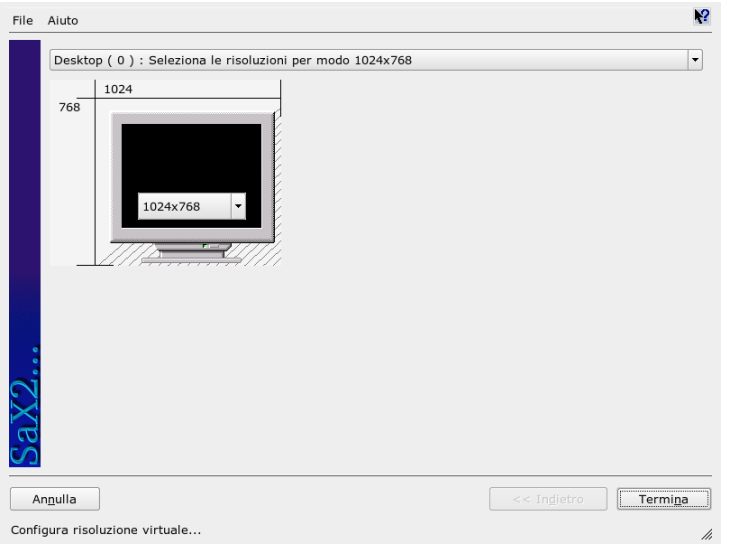

Figura 11.5: *Impostare la risoluzione virtuale*

11.1.7 Multihead

Se il vostro sistema presenta più di una scheda grafica o una scheda con più uscite, potete connettere più schermi al vostro sistema. Con due schermi, avrete un sistema *dualhead*, mentre con più di due, si ha un sistema *multihead*. SaX2 riconosce automaticamente la presenza di più schede e adatta la configurazione di conseguenza. Nella finestra multihead potete fissare il modo multihead e la disposizione degli schermi. Potete scegliere tra tre modi: 'Tradizionale' (default), 'Xinerama' e 'Cloned':

Multihead tradizionale Ogni monitor rappresenta un'unità a sé stante. Il mouse può passare da uno schermo all'altro.

Cloned Multihead Qui tutti i monitor visualizzano lo stesso contenuto ed il mouse è visibile solo sullo schermo principale.

Xinerama Multihead Tutti gli schermi vengono "fusi" in uno grande, le finestre dei programmi possono essere posizionati su uno schermo qualsiasi o ingrandite fino a riempire tutti i monitor.

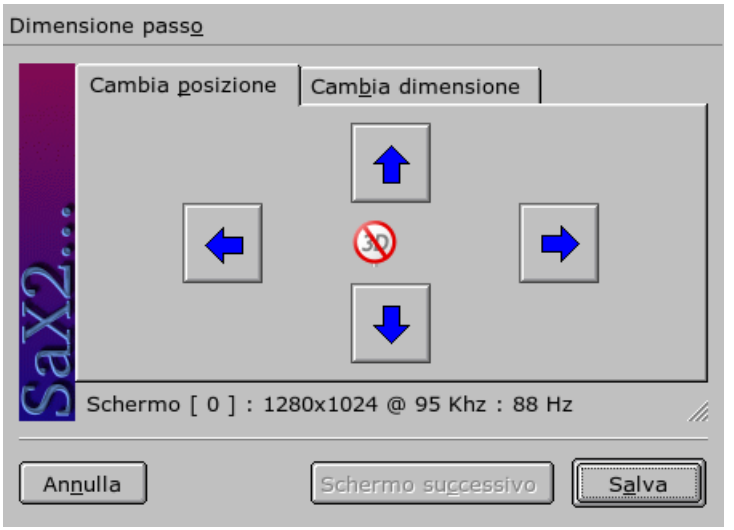

Figura 11.6: *Modificare la geometria dello schermo*

Il "layout" di un ambiente multihead è la disposizione degli schermi ed il rapporto che intercorre tra i singoli schermi. SaX2 assegna un layout standard che si attiene alla sequenza delle schede grafiche rilevate. Gli schermi risulteranno allineati da sinistra a destra. Nel dialogo 'Layout' dello strumento di configurazione multihead, impostate l'ordine dei monitor spostando con il mouse i simboli degli schermi nella griglia. Chiudete il dialogo di Layout e testate la configurazione degli schermi cliccando sul pulsante 'Test'.

Vi preghiamo di tenere presente che Linux, al momento, non supporta il 3D in ambienti Xinerama Multihead. In questo caso, pertanto, SaX2 disattiva automaticamente il supporto 3D.

11.1.8 Dispositivi di immissione

Mouse Se il dispositivo non è stato rilevato in modo automatico, configurate il mouse manualmente, aiutandovi con la descrizione contenuta nella documentazione del mouse. Selezionate il tipo di mouse dalla lista dei modelli supportati e confermate con un clic del tasto ⑤ del tastierino numerico.

Tastiera In questo dialogo, impostate il tipo di tastiera nel campo di selezione in alto. Scegliete anche la lingua della tastiera (ovvero la mappatura dei tasti del vostro paese). Testate poi il funzionamento della configurazione, digitando dei caratteri speciali, come “à” o “è”.

Lasciate la casella di attivazione delle vocali accentate come preimpostata per la vostra lingua. Salvate la configurazione con ‘Fine’.

Schermo tattile X.Org supporta, al momento, i touchscreen della Microtouch e Elo TouchSystems. SaX2 riconosce automaticamente solo il monitor, ma non il toucher, che va visto a sua volta come un dispositivo di immissione.

Per configurare il toucher avviate SaX2 e passate a ‘Dispositivi di immissione’ → ‘Schermo tattile’. Cliccate su ‘Aggiungi’ ed aggiungete un touchscreen. Salvate la configurazione con un clic su ‘Fine’. Non è necessario testare la configurazione.

I touchscreen sono molto versatili e, nella maggior parte dei casi, devono essere prima calibrati. Linux, purtroppo, non offre ancora alcuno strumento per calibrare dei touchscreen. La configurazione standard include buoni parametri di default per le dimensioni del touchscreen, di modo che solitamente non sono necessarie ulteriori impostazioni.

Tavola grafica X.Org attualmente supporta un numero limitato di tavole grafiche. SaX2 vi permette di configurare tavole grafiche connesse alla porta USB o seriale. Dal punto di vista della configurazione, una tavola grafica equivale ad un mouse vi consigliamo di procedere come segue:

Avviate SaX2 e passate a ‘Dispositivi di immissione’ → ‘Tavola grafica’. Cliccate su ‘Aggiungi’, selezionate nel dialogo la casa produttrice del dispositivo e aggiungete una tavola grafica dalla lista che vi viene mostrata. Eventualmente, spuntate le check box a destra se avete connesso una penna o cancellino. Se la tavola è connessa alla porta seriale, verificatene la connessione: `/dev/ttyS0` è la prima interfaccia seriale, `/dev/ttyS1` la seconda e via di seguito. Salvate la configurazione, cliccando su ‘Fine’.

11.1.9 AccessX

Se lavorate al vostro sistema senza ricorrere al mouse, avviate SaX2 ed attivate AccessX per poter spostare il puntatore del mouse sul vostro schermo con il tastierino numerico (si veda la tabella 11.1 nella pagina successiva per una descrizione delle funzioni dei vari tasti). Tramite la levetta (ingl. slider) impostate la velocità di movimento del puntatore.

Tabella 11.1: *AccessX: muovere il mouse tramite il tastierino numerico*

Tasto	Descrizione
(÷)	Seleziona il tasto sinistro del mouse
(x)	Seleziona il tasto centrale del mouse
(–)	Seleziona il tasto destro del mouse
(5)	Questo tasto esegue un clic del tasto di mouse abilitato in precedenza. Se non avete abilitato alcun tasto di mouse, viene utilizzato il tasto sinistro. Lo stato di abilitazione del tasto in questione dopo il clic viene riportato allo stato preimpostato.
(+)	Questo tasto ha lo stesso effetto di (5), con la differenza che aziona un doppio clic.
(0)	Questo tasto ha la stessa funzione di (5), con la differenza che corrisponde al tenere premuto il tasto del mouse.
(Canc)	Questo tasto "rilascia" il tasto del mouse (che era tenuto premuto dal tasto (0)).
(7)	Muove il mouse verso l'alto, a sinistra.
(8)	Muove il mouse verso l'alto, in linea retta.
(9)	Muove il mouse verso l'alto, a destra.
(4)	Muove il mouse verso sinistra
(6)	Muove il mouse verso destra
(1)	Muove il mouse verso il basso, a sinistra
(2)	Muove il mouse verso il basso, in linea retta
(3)	Muove il mouse verso il basso, a destra

11.1.10 Joystick

Questo modulo vi permette di configurare il vostro joystick selezionando dall'elenco il produttore e modello. 'Prova' vi permette di verificare il corretto funzion-

ameno del vostro joystick. La finestra della prova vi mostra tre diagrammi per le assi analoghe del joystick e dei simboli per i quattro pulsanti standard. Quando muovete il joystick o premete i pulsanti, la reazione viene visualizzata nella finestra del test. Visto che i joystick di solito sono connessi alla scheda audio, questo modulo può essere invocato anche dalla finestra di configurazione della scheda audio.

11.2 Ottimizzare la configurazione del sistema X Window

"X.Org" rappresenta un'implementazione a sorgente aperto dell' X Window system. "X.Org Foundatation", che nel contempo è responsabile per lo sviluppo di nuove tecnologie e standard dell' X Window Systems, porta avanti lo sviluppo di questa implementazione.

Per poter utilizzare in modo ottimale l'hardware a disposizione (mouse, scheda grafica, schermo, tastiera) vi è la possibilità di ottimizzare la configurazione manualmente. Illustreremo alcuni aspetti del modo di applicare le ottimizzazioni. Per delle informazioni dettagliate riguardanti la configurazione dell'X Window System consultate i file nella directory `/usr/share/doc/packages/Xorg` nonché chiaramente la pagina di manuale con: `man xorg.conf`.

Avvertimento

Durante il processo di configurazione dell'X Window Systems si dovrebbe procedere con cautela! Non lanciate X11 prima che ne sia stata terminata la configurazione. Un sistema impostato in modo errato può causare dei danni irriparabili al vostro hardware; particolare attenzione va fatta con schermi a frequenza fissa. Gli autori del presente manuale e SUSE LINUX declinano ogni responsabilità per danni che eventualmente potrebbero verificarsi. Il presente testo è stato redatto con la massima accuratezza possibile, comunque non si può garantire che i metodi qui presentati siano esenti da errori, quindi non si può escludere che venga danneggiato il vostro hardware.

Avvertimento

I programmi SaX2 e xf86config creano il `xorg.conf` di default in `/etc/X11`. Questo è il file di configurazione primario dell' X Window System. Qui trovate le indicazioni sul mouse, schermo e scheda grafica.

In questa sezione descriveremo la struttura del file di configurazione `/etc/X11/xorg.conf`. Questo file è suddiviso in sezioni (ingl. sections) introdotte dalla parola chiave `Section "identificatore"`, che terminano con `EndSection`. Ci limiteremo a presentare le sezioni principali.

`xorg.conf`, come già accennato, è composto da più `Sections`, ognuna delle quali si occupa di un aspetto particolare della configurazione. Una sezione è sempre strutturata nel modo seguente:

```
Section designazione
registrazione 1
registrazione 2
registrazione n
EndSection
```

Le sezioni disponibili sono riportati nella tabella 11.2 in questa pagina.

Tabella 11.2: *Sezioni in /etc/X11/xorg.conf*

Tipo	Significato
`Files`	Questa sezione descrive i percorsi usati per i font e le tabelle cromatiche RGB.
`ServerFlags`	Qui vengono indicati i server flag.
`InputDevice`	Tramite questa sezione vengono configurati i dispositivi d'immissione, ovvero tastiere, mouse e speciali dispositivi di immissione come schermi tattili, joystick etc. Gli indicatori importanti sono qui `Driver` e le opzioni che stabiliscono `Protocol` e `Device`.
`Monitor`	Descrive il monitor utilizzato. Gli elementi di questa sezione sono: il nome, a cui si rimanda per la definizione degli `Screens`, la descrizione della larghezza di banda (`Bandwidth`) e delle frequenze di sincronizzazione consentite (`HorizSync` e `VertRefresh`). Le indicazioni sono espresse in MHz, kHz o Hz. Fondamentalmente il server rifiuta ogni modeline che non corrisponda alle specifiche del monitor: in questo modo si evita che, facendo esperimenti con le modeline, possano venire inviate al monitor frequenze troppo alte.

`Modes`	Qui vengono definiti i parametri delle modeline per le varie risoluzioni dello schermo. Questi parametri possono venire calcolati da SaX2 in base ai valori indicati dall'utente e generalmente non devono venire modificati. Potete però intervenire manualmente se per esempio intendete collegare uno schermo a frequenza fissa. Una illustrazione dettagliata dei singoli valori numerici la trovate nel file HOWTO `/usr/share/doc/howto/en/XFree86-Video-Timings-HOWTO.gz`.
`Device`	Questa sezione definisce una determinata scheda grafica. Ci si riferisce ad essa tramite il nome descrittivo.
`Screen`	Questa sezione infine unisce un `Monitor` e un `Device` da cui derivare le indicazioni necessarie per X.Org. La sottosezione `Display` permette di indicare la dimensione virtuale dello schermo (`Virtual`), del `ViewPort` e dei `Modes` usati con questo schermo.
`ServerLayout`	Questa sezione definisce il layout di una configurazione singlehead o multihead. Qui vengono raggruppati i dispositivi d'immessione `InputDevice` e quelli di visualizzazione. `Screen`.

Occupiamoci ora delle sezioni `Monitor`, `Device` e `Screen`. Nella pagina di manuale di `X.Org` e `xorg.conf` troverete ulteriori informazioni sulle altre sezioni.

Un file `xorg.conf` può contenere una serie di sezioni `Monitor` e `Device`. Sono possibili anche più sezioni `Screen`; quale di queste venga usata, dipende dalla sezione successiva `ServerLayout`.

11.2.1 Sezione Screen

Diamo un'occhiata alla sezione screen; come già accennato, questa combina una sezione monitor e una device, stabilendo la risoluzione e la profondità dei colori. Ecco una sezione screen esempio 11.1 nella pagina successiva.

Esempio 11.1: *La sezione Screen del file /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 riga `Identifier` (qui `Screen[0]`) dà a questa sezione una denominazione univoca, attraverso la quale nella sezione successiva `ServerLayout` si potrà fare riferimento ad essa in modo univoco. Tramite le voci `Device` e `Monitor` vengono assegnati a `Screen` in modo univoco la scheda grafica e monitor. Si tratta di semplici riferimenti alle sezioni `Device` e `Monitor` con i rispettivi nomi o *identifiers*. Entreremo nei dettagli riguardanti queste sezioni più avanti.

Tramite l'indicazione `DefaultDepth` si può scegliere con quale profondità del colore debba partire il server (se non viene inizializzato con una precisa indicazione della profondità del colore). Per ogni profondità di colore segue una sottosezione `Display`. La profondità di colore per la quale è valida la sottosezione, viene stabilita dalla parola chiave `Depth`. I valori possibili per `Depth` sono 8, 15, 16 e 24. Non tutti i moduli dell'X server supportano ognuno di questi valori.

Dopo la profondità di colore, con `Modes` viene stabilita una serie di risoluzioni che l'X server leggerà da sinistra a destra. Per ogni risoluzione viene cercata nella sezione `Modes` un `Modeline`. `Modeline` dipende dalla caratteristiche del monitor e scheda grafica. Le impostazioni `Monitor` determinano il `Modeline` risultante.

La prima risoluzione rilevata è il `Default-Mode`. Con i tasti Ctrl-Alt-(+) (del tasterino numerico) vi spostate a destra, con i tasti Ctrl-Alt-(-) (sul tasterino numerico) a sinistra. In questo modo si può variare la risoluzione dello schermo con il sistema X-Window in esecuzione.

L'ultima riga della sottosezione `Display` con `Depth 16` si riferisce alla dimensione dello schermo virtuale. La dimensione massima dello schermo virtuale dipende dalla quantità di memoria della scheda video e dalla profondità di colore desiderata, e non dalla risoluzione massima del monitor. Dato che le recenti schede grafiche dispongono di tanta memoria grafica, si possono generare desktop virtuali di notevole dimensioni. Tenete presente però che eventualmente non potrete più utilizzare le funzionalità tridimensionali se in pratica riempite l'intera memoria grafica con un desktop virtuale. Se p.es. la scheda grafica ha 16 Mbyte di video RAM, lo schermo virtuale - con una profondità di colore di 8 bit - può raggiungere fino a 4096x4096(!) pixel. Specialmente con schede accelerate non è consigliabile dedicare allo schermo virtuale l'intera memoria della scheda grafica, poiché la memoria viene allocata anche per diverse cache grafiche e dei font.

11.2.2 Device-Section

Una Device Section descrive e definisce una determinata scheda grafica. `xorg.conf` può contenere diverse sezioni del genere, sempre che il loro nome, il quale viene indicato dalla parola chiave `Identifier`, sia diverso. In genere, se avete integrato nel sistema più di una scheda grafica, le sezioni vengono numerate, la prima con `Device[0]`, la seconda con `Device[1]` etc. Ecco un estratto della sezione `Device` di un computer con una scheda grafica Matrox Millennium PCI:

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

Se per la configurazione usate SaX2, la device section dovrebbe corrispondere più o meno a quella riportata sopra. In particolar modo le voci `Driver` e `BusID` dipendono dall'hardware installato e vengono rilevate automaticamente da SaX2. `BusID` determina lo slot PCI o AGP della scheda grafica che corrisponde all'ID

emessa dal comando lspci. Tenete presente che l'X server richiede le indicazioni nel modo decimale, mentre il programma lspci le emette in modo esadecimale!

Tramite il parametro `Driver` stabilite il driver da usare per questa scheda grafica. Nel caso della Matrox Millennium, il modulo driver si chiama `mga`. L'X server li cerca in `ModulePath`\definito nella sezione `Files` nella sottodirectory `drivers`. In una installazione standard, la directory è `/usr/X11R6/lib/modules/drivers`; al nome viene semplicemente aggiunto `_drv.o`; nel caso del driver `mga` viene caricato quindi il file driver `mga_drv.o`.

Tramite ulteriori opzioni, è possibile influenzare il comportamento dell'X server o del driver. Nella device section vi è ad esempio impostata l'opzione `sw_cursor`, che disattiva il cursore hardware del mouse e abilita quello software. A seconda del modulo driver, avete a disposizione diverse opzioni descritte nei file documentazione che trovate nella directory `/usr/X11R6/lib/X11/doc`. Opzioni valide in modo generale si trovano anche nelle rispettive pagine di manuale (`man xorg.conf` e `man`X.Org).

11.2.3 Monitor Section e Modes Section

Analogamente alle sezioni `Device`, le sezioni `Monitor` e sezioni `Modes` descrivono e definiscono un determinato monitor. Il file di configurazione `/etc/X11/xorg.conf` può contenere un numero qualsiasi di sezioni `Monitor` che devono avere tutte nomi diversi. Nella sezione ServerLayout viene stabilito quale sezione `Monitor` sia quella rilevante.

Per la definizione del monitor vale, ancor più che per la descrizione della scheda grafica, che solamente utenti esperti dovrebbero creare una sezione `Monitor` (e questo vale in particolar modo per la sezione modes). I componenti principali della sezione Modes sono le modeline che indicano il timing orizzontale e verticale per la rispettiva risoluzione. Nella sezione `Monitor` vengono registrate le proprietà del monitor e specialmente le frequenze di deflessione consentite.

Avvertimento

Senza cognizioni di base sul funzionamento di monitor e scheda grafica, non si dovrebbero modificare le modeline, poiché ciò potrebbe danneggiare seriamente il vostro monitor!

Avvertimento

Chi desidera generare una propria descrizione del monitor, dovrebbe prima leggere la documentazione contenuta nella directory `/usr/X11/lib/X11/doc`. In

particolar modo da sottolineare è la parte che tratta i video modes in cui viene descritto il modo in cui funziona l'hardware e come creare le modeline.

Fortunatamente, diventano sempre più rari i casi in cui bisogna impostare manualmente le modeline o le definizioni monitor. Se usate un moderno monitor multisync di solito l'X server sarà in grado di leggere gli intervalli di frequenza consentiti e la risoluzione ottimale (come già accennato nella sezione di configurazione SaX2) del monitor direttamente per via del DDC. Se ciò non dovesse essere possibile, potete usare uno dei modi VESA integrato dell'X server. Questi dovrebbero funzionare perfettamente con ogni combinazione di schede grafiche e monitor.

11.3 Installare e configurare dei font

Installare ulteriori font sotto SUSE LINUX è molto semplice; basta copiare i font in una directory qualsiasi che si trovi nel percorso del font X11 (si veda la sezione 11.3.2 a pagina 244), Per fare in modo che i font siano utilizzabili anche tramite il nuovo sistema di font rendering Xft, la directory di installazione dovrebbe essere una una sottodirectory delle directory configurate in `/etc/fonts/fonts.conf` (si veda la sezione 11.3.1 nella pagina successiva).

Come utente `root` si possono copiare manualmente i file del font in una directory indicata, per esempio in `/usr/X11R6/lib/X11/fonts/truetype`, oppure potrete utilizzare a tal fine anche il font installer di KDE che trovate nel centro di controllo di KDE. Il risultato è identico.

Invece di copiare i font vi è inoltre la possibilità di creare dei link simbolici, se ad es. avete un font (con licenza) su una partizione Windows montata e volete utilizzarlo. In seguito invocate `SuSEconfig --module fonts`.

`SuSEconfig --module fonts` inizializza lo script `/usr/sbin/fonts-config` che esegue la configurazione dei font. Per maggiori dettagli su quanto esegue lo script leggete la relativa pagina di manuale (`man fonts-config`).

Non fa differenza quale tipo di font dovrà essere installato la procedura è sempre la stessa, sia che si tratti di font bitmap, font TrueType/OpenType e font Type1-(PostScript). Tutti questi tipi di font possono essere installati in una directory qualunque. L'unica eccezione è rappresentato dal font CID-keyed, si veda la sezione 11.3.3 a pagina 245.

X.Org contiene due sistemi di font completamente differenti, il vecchio *sistema di font X11 Core* ed il nuovo sistema *Xft/fontconfig*. Segue una breve descrizione dei due sistemi.

11.3.1 Xft

In fase di ideazione di Xft l'accento è stato posto sul supporto di font scalabili, incluso l'anti-aliasing. Con Xft i font vengono modificati dal programma che utilizza i font e non dall' X server come era invece il caso con il font system Core di X11. In questa maniera il programma in questione guadagna l'accesso ai file del font ed il pieno controllo sul modo di resa dei glifi. Questo permette la rappresentazione di testo corretta nelle varie lingue, inoltre l'accesso diretto ai file di font è di aiuto per integrare (ingl. to embed) font per il processo di stampa, affinché quanto emesso allo schermo corrisponda effettivamente a quanto emesso dalla stampante.

In SUSE LINUX i due ambienti desktop KDE e Gnome, Mozilla e tante altre applicazioni utilizzano già Xft di default. Quindi, Xft viene utilizzato già da più applicazioni che il vecchio sistema di font X11 Core.

Xft utilizza la libreria fontconfig per trovare i font e per influire sul rendering. Il comportamento di fontconfig viene regolato da un file di configurazione valido per l'intero sistema `/etc/fonts/fonts.conf` e da un file di configurazione dell'utente `~/.fonts.conf`. Ogni file di configurazione di fontconfig deve iniziare con

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

e terminare con

```
</fontconfig>
```

Per aggiungere delle directory dove cercare dei font, aggiungete una riga simile a questa

```
<dir>/usr/local/share/fonts/</dir>
```

Ciò sarà necessario solo di rado; la directory dell'utente `~/.fonts` è già registrata in `/etc/fonts/fonts.conf` di default. Se un utente desidera installare ulteriori font, basta copiarli in `~/.fonts`.

Potete anche inserire delle regole per determinare l'aspetto dei font, ad esempio

```
 <match target="font">
 <edit name="antialias" mode="assign">
 <bool>false</bool>
 </edit>
</match>
```

per disattivare l'anti-aliasing per tutti i font, oppure

```
<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>
```

se si vuole disattivarlo solo per determinati font.

La maggioranza delle applicazioni utilizzano di default i nomi di font `sans-serif` (o l'equivalente `sans`), `serif` o `monospace`. Si tratta di font che non esistono effettivamente, ma di soli alias che vengono risolti, in base alla lingua impostata, in un font appropriato.

Ogni utente potrà aggiungere delle regole nel suo `~/.fonts.conf` visto questi alias vengono risolti nei suoi font di preferenza:

```
  <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>
```

Dato che quasi tutte le applicazioni utilizzano di default questi alias, questo influisce su tutto il sistema. In tal maniera con il minimo sforzo potete utilizzare i vostri font preferiti quasi dappertutto senza dovere intervenire singolarmente sull'impostazione dei font in ogni programma.

Per vedere quali font sono installati e disponibili, vi è il comando `fc-list`. Ad esempio `fc-list ""` emette un elenco di tutti i font. Se volete sapere quali sono i font scalabili a vostra disposizione (`:outline=true`) che contengono tutti i glifi richiesti per l'ebraico (`:lang=he`) il loro nome di font (`family`), il loro stile (`style`), e grado di grassetto (`weight`) ed il nome dei file contenenti i font, immettete ad esempio il seguente comando:

```
fc-list ":lang=he:outline=true" family style weight file
```

Ecco come potrebbe essere l'output di questo comando:

```
/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
```

Ecco i principali parametri che possono venire elencati con `fc-list`:

Tabella 11.3: *Possibili parametri di fc-list*

Parametri	Significato e valori possibili
`family`	Il nome della famiglia di font ad esempio `FreeSans`
`foundry`	I produttori del font ad esempio `urw`
`style`	Lo stile di font ad esempio `Medium`, `Regular`, `Bold`, `Italic`, `Heavy`.
`lang`	La/le lingua/e supportata/e dal font. Ad esempio `de` per tedesco, `ja` per il giappone, `zh-TW` per il cinese tradizionale, `zh-CN` per il cinese semplificato.
`weight`	Il *grado di grassetto*, ad esempio `80` non in grassetto, `200` in grassetto.

`slant`	Il *grado della corsività*, spesso `0` non corsivo, `100` in corsivo.
`file`	Il nome del contenente il font.
`outline`	`true` se si tratta di un font cosiddetto outline, altrimenti `false`.
`scalable`	`true` se si tratta di un font scalabile, altrimenti `false`.
`bitmap`	`true` se si tratta di un font bitmap, altrimenti `false`.
`pixelsize`	La dimensione del font in pixel. Assieme a fc-list indicato solo per font bitmap.

11.3.2 Font X11 Core

Oramai il sistema di font X11 core non supporta solo font bitmap, ma anche font scalabili come font Type1, TrueType/OpenType e font CID-keyed. Anche font Unicode vengono supportati già da parecchio tempo. Nel 1987 il sistema di font X11 Core è stato sviluppato per X11R1 per poter elaborare font bitmap monocromatici. Tutte le estensioni menzionate sopra sono state aggiunte in un secondo momento.

Font scalabili vengono supportati solo senza antialiasing e subpixel rendering; caricare cospicui font scalabili con glifi per numerose lingue può rilevarsi un processo molto lento. Anche l'utilizzo di font unicode può richiedere molto tempo e tanta memoria.

Vi sono anche altri punti deboli del sistema di font X11 Core e si può tranquillamente asserire che si tratta di un font ormai passé non più estendibile in modo proponibile. Comunque per motivi di compatibilità con versioni precedenti rimane disponibile, ma dove possibile si dovrebbe utilizzare il sistema più moderno Xft/fontconfig.

L' X server deve sapere quali font sono disponibili e dove trovarli. La variabile FontPath svolge questa funzione, essa contiene il percorso di tutte le directory dei font di sistema validi. Ognuna di queste directory ha un file denominato `fonts.dir` che elenca i font disponibili nella directory. FontPath viene generata dall'X server all'avvio con il compito di trovare un file `fonts.dir` valido in ogni registrazione `FontPath` del file di configurazione `/etc/X11/xorg.conf`. Queste registrazioni si trovano nella sezione `Files`. Il comando `xset q` visualizza il FontPath. xset permette di modificare questo percorso anche con il sistema in esecuzione. Per aggiungere dei percorsi eseguite `xset +fp <percorso>`, e per eliminare dei percorsi indesiderati eseguite `xset -fp <percorso>`.

Se l' X server è già in esecuzione potete rendere disponibili font appena installati nelle directory montate, ossia integrate nel file system, tramite il comando: `xset fp rehash`. Questo comando viene invocato già da `SuSEconfig --module fonts`. Dato che il comando `xset` richiede l'accesso all'X server in esecuzione, ciò funzionerà solo se `SuSEconfig --module fonts` è stato lanciato da una shell con accesso ad un X server in esecuzione. Il modo più semplice per realizzare ciò consiste nell'immissione del comando `su` seguito dall'immissione del password di root in un terminale per diventare `root`, `su` passerà i permessi di accesso dell'utente che ha lanciato l'X server alla root shell. Per verificare se i font sono stati installati in modo corretto e la loro disponibilità tramite il sistema di font X11 core utilizzate il comando `xlsfonts` per avere un elenco di tutti i font disponibili.

SUSE LINUX utilizza di default locales UTF-8, quindi dovreste utilizzare font Unicode che si riconoscono dalla desinenza `iso10646-1` nell'output di `xlsfonts`. Tutti i font Unicode disponibili possono essere visualizzati anche con `xlsfonts | grep iso10646-1`. Quasi tutti i font Unicode forniti a corredo con SUSE LINUX contengono almeno tutti i glifi necessari per le lingue europee per cui si utilizzava in passato l'encoding `iso-8859-*`.

11.3.3 Font CID-keyed

A differenza di altri tipi di font, i font CID-keyed non possono essere installati in una directory qualunque, vanno installati sotto `/usr/share/ghostscript/Resource/CIDFont`. Questo non fa differenza per Xft/fontconfig, ma lo richiedono Ghostscript ed il sistema di font X11 Core.

Suggerimento

Per ulteriori informazioni in tema di font sotto X11 consultate `http://www.xfree86.org/current/fonts.html`.

Suggerimento

11.4 Configurare OpenGL/3D

11.4.1 Supporto hardware

SUSE LINUX include molti driver OpenGL per il supporto hardware 3D. Ecco una rassegna nella tabella 11.4 nella pagina successiva.

Tabella 11.4: *Hardware 3D supportato*

Driver OpenGL	Hardware supportato
nVidia	Chip nVidia: tutti tranne 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 (fino a 9250)

Se effettuate l'installazione tramite YaST, potete attivare il supporto 3D già durante l'installazione, se sono date le premesse. Nel caso dei chip grafici nVidia si deve installare innanzitutto il driver nVidia. Selezionate a riguardo durante il processo di installazione la patch del driver nVidia in YOU (YaST Online Update). Per motivi di licenza, purtroppo non ci è consentito accludere il driver nVidia.

Se eseguite un update o dovete impostare una scheda grafica aggiuntiva 3Dfxi (Voodoo Graphics o Voodoo-2) la procedura cambia. In tema di supporto supporto hardware 3D tutto dipende dal driver OpenGL utilizzato. Per maggiori dettagli proseguite nella lettura.

11.4.2 Driver OpenGL

I driver OpenGL nVidia e DRI possono essere configurati comodamente con SaX2. Tenete presente per una scheda nVidia va installato innanzitutto il driver nVidia. Con il comando `3Ddiag`, potete verificare la correttezza della configurazione di nVidia o DRI.

Per ragioni di sicurezza, solo gli utenti appartenenti al gruppo `video` possono accedere all'hardware 3D. Accertatevi che tutti gli utenti che lavorano localmente sul computer appartengano a questo gruppo. In caso contrario, per le applicazioni OpenGL si ripiegherà sul *software rendering fallback* del driver OpenGL che è più lento. Usate il comando `id` per verificare se l'utente attuale appartiene al gruppo `video`. Se non appartiene al gruppo, potete usare YaST per aggiungere l'utente al gruppo.

11.4.3 Tool di diagnosi 3Ddiag

Per controllare la configurazione 3D su SUSE LINUX vi è lo strumento di diagnosi 3Ddiag. Si tratta di uno strumento a riga di comando che deve essere invocato da un terminale. Eseguite `3Ddiag -h` per avere le opzioni ammesse per 3Ddiag.

Per verificare la configurazione di X.Org, questo tool controlla se sono installati i pacchetti richiesti per il supporto 3D e se viene utilizzata la corretta libreria OpenGL e le corrette estensioni GLX. Seguite le istruzioni di 3Ddiag se vengono visualizzati dei messaggi failed. Se tutto è andato per il verso giusto verranno visualizzati solo messaggi done.

11.4.4 Testare OpenGL

A tal fine possono essere usati accanto a `glxgears` giochi come `tuxracer` e `armagetron` (pacchetti omonimi). Se il supporto 3D è stato attivato, tali giochi dovrebbero essere giocabili in modo abbastanza fluido su un computer relativamente recente. Senza supporto 3D ciò non ha senso (effetto moviola). Per vedere se l'accelerazione 3D è abilitata o meno, utilizzate il comando `glxinfo`: se l'output presenta un rigo con `direct rendering: Yes`, allora tale funzionalità è abilitata.

11.4.5 Risoluzione di alcuni possibili problemi

Se i risultati dei test a cui è stato sottoposto OpenGL 3D lasciano a desiderare (impossibile giocare in modo fluido), usate 3Ddiag per assicurarvi che non vi siano degli errori di configurazione (messaggi `failed`) ed eventualmente eliminateli. Se ciò non è di aiuto o non vi sono dei messaggi failed, date un'occhiata al file di log di X.Org.

Spesso troverete la riga `DRI is disabled` in `/var/log/Xorg.0.log`. L'esatta causa del problema può essere individuata solo analizzando attentamente il file di log, compito che a volta si rivela troppo difficile per un neofita.

In questi casi, spesso non vi sono degli errori di configurazione, poiché questi ultimi sarebbero già stati rilevati da 3Ddiag. Perciò, a questo punto, non rimane che il software rendering fallback del driver DRI, che purtroppo non offre supporto per l'hardware 3D. Si dovrebbe rinunciare al supporto 3D se vi sono degli errori di rappresentazione OpenGL o addirittura problemi di instabilità. Utilizzate SaX2 per disabilitare il supporto 3D.

11.4.6 Supporto all'installazione

A parte il `software rendering fallback` del driver DRI, in Linux tutti i driver OpenGL si trovano in fase di sviluppo e devono pertanto essere considerati in parte sperimentali. I driver sono inclusi nella distribuzione perché c'è una forte richiesta di funzionalità 3D sotto Linux. Considerando lo stato in parte sperimentale dei driver OpenGL, non possiamo però offrire alcun supporto all'installazione per la configurazione dell'accelerazione hardware 3D o fornire qualsiasi ulteriore assistenza per difficoltà in questo contesto. La configurazione di base dell'interfaccia utente grafica (X Window System) non include la configurazione dell'accelerazione hardware 3D. Speriamo comunque che questo capitolo fornisca una risposta a molte domande relative a questo argomento. Se avete delle difficoltà con il supporto hardware 3D, consigliamo in caso di dubbio di rinunciare al supporto 3D.

11.4.7 Ulteriore documentazione in linea

Per delle informazioni su DRI, consultate `/usr/X11R6/lib/X11/doc/README.DRI` (`xorg-x11-doc`). Per maggiori informazioni sull'installazione di driver nvidia rimandiamo al sito `http://ftp.suse.com/pub/suse/i386/supplementary/X/nvidia-installer-HOWTO.html`.

Processo di stampa

Il presente capitolo illustrerà le varie fasi che compongono il processo di stampa con l'obiettivo di far luce anche sui modi di risolvere eventuali difficoltà che potrebbero sorgere durante il processo di stampa.

12.1 Preliminari e ulteriori considerazioni

CUPS è il sistema di stampa di default di SUSE LINUX. CUPS si orienta in prima linea all'utente. In molti casi è compatibile con LPRng o può venir reso tale in modo piuttosto semplice. LPRng è incluso in SUSE LINUX solo per ragioni di compatibilità.

Le stampanti si possono distinguere in base all'interfaccia (USB, rete) o in base al linguaggio della stampante. Quando acquistate una stampante l'attenzione va posta sul supporto da parte dell'hardware per quel che riguarda l'interfaccia e sul linguaggio della stampante. Da un punto di vista del linguaggio le stampanti si lasciano suddividere nelle seguenti tre categorie:

Stampanti PostScript PostScript è il linguaggio di stampa maggiormente diffuso sotto Linux/Unix. Si tratta di un linguaggio molto potente che esiste già da parecchio tempo. Se documenti PostScript vengono elaborati direttamente dalla stampante, quindi senza che lo debbano essere dal sistema di stampa interno, si lascia ridurre il numero delle cause possibili di errore. Visto che vi è una licenza dal costo non trascurabile per stampanti PostScript, il prezzo di queste stampanti è generalmente superiore a quello di stampanti sprovviste di un cosiddetto interpreter PostScript.

Linguaggi di stampa standard come ad es. PCL e ESC/P
Si tratta di linguaggi che esistono già da parecchio tempo ma che ancor oggi vengono adattati in modo da poter gestire anche funzionalità di stampanti più recenti. Nel caso di linguaggi di stampa noti, il sistema di stampa è in grado di convertire incarichi PostScript nel rispettivo linguaggio di stampa ricorrendo a Ghostscript. Tra i linguaggi più noti vi è PCL, utilizzato soprattutto da stampanti HP e dai suoi "clone", e ESC/P utilizzato da stampanti Epson. Con questi linguaggi si ottengono anche sotto Linux dei buoni risultati per quel che riguarda le stampe. Può verificarsi il caso che Linux non supporti almeno per un certo lasso di tempo determinate funzionalità di stampanti recentissime e un pò stravaganti per il fatto che gli sviluppatori della comunità Open Source hanno i lavori in corso e sono impegnati a trovare il modo di supportarle. Fatta eccezione per i driver `hpijs` che vengono sviluppati dalla stessa HP, attualmente non vi è alcun produttore di stampanti che sviluppi driver Linux e che li rilasci sotto una licenza open source mettendoli a disposizione delle distribuzioni Linux. Da un punto di vista del prezzo per questo tipo di stampanti ci muoviamo nel segmento medio.

Stampanti proprietarie, solitamente stampanti GDI
: Per le stampanti proprietarie vi è spesso solo uno oppure anche diversi driver Windows. Questo tipo di stampante non si basa su un linguaggio di stampa noto ed inoltre il linguaggio di stampa può cambiare da un modello all'altro. Come affrontare la problematica viene illustrato nella sezione 12.8.1 a pagina 266.

Prima di acquistare una nuova stampante si dovrebbero consultare le seguenti fonti di informazione per vedere se il dispositivo che si intende acquistare venga supportato da Linux o meno:

- `http://cdb.suse.de/` — la banca dati di SUSE LINUX in tema di stampanti
- `http://www.linuxprinting.org/`—— la banca dati di stampanti LinuxPrinting.org
- `http://www.cs.wisc.edu/~ghost/` — il sito web di Ghostscript
- `/usr/share/doc/packages/ghostscript/catalog.devices`— i driver inclusi

Chiaramente le banche dati online sono aggiornatissime in tema di supporto Linux, mentre un prodotto può includere solo dei driver disponibili al momento della sua produzione; quindi possono verificarsi delle discrepanze, ossia una stampante classificata come "perfettamente supportata" potrebbe non esserlo stata al momento del rilascio dell'ultima versione di SUSE LINUX. Le banche dati quindi non rispecchiano sempre lo stato effettivo delle cose, si tratta piuttosto di una buona approssimazione.

12.2 Sistema di stampa: flusso di lavoro

L'utente crea un incarico di stampa. L'incarico di stampa si compone dei dati da stampare e in più le informazioni destinate allo spooler, tipo il nome della stampante o il nome della coda di stampa e facoltativamente le informazioni per il filtro, vale a dire particolari opzioni della stampante.

Per ogni stampante vi è una coda di stampa dedicata. Lo spooler mantiene l'incarico di stampa nella coda di stampa finché la stampante prescelta è pronta a

ricevere i dati. Quando la stampante è pronta, lo spooler invia i dati tramite il filtro e back-end alla stampante.

Il filtro converte i dati che l'utente intende stampare (ASCII, PostScript, PDF, JPEG, etc.) in dati processabili per la stampante (PostScript, PCL, ESC/P, etc.). Le funzionalità della stampante vengono descritte nei file PPD. Un file PPD contiene le opzioni specifiche di una stampante con i parametri richiesti per abilitarle nella stampante. Il sistema di filtraggio fa sì che le opzioni selezionate da parte dell'utente siano abilitate.

Se utilizzate una stampante PostScript, il sistema di filtraggio della stampante converte i dati in dati elaborabili dalla stampante PostScript. In questo caso non è richiesto un driver della stampante. Se siete in possesso di una stampante non-PostScript, il sistema di filtraggio converte i dati in dati processabili per la stampante tramite Ghostscript. Questo processo richiede un driver di stampante Ghostscript adatto alla vostra stampante. Il back-end riceve i dati specifici della stampante e li inoltra alla stampante.

12.3 Connessione della stampante: metodi e protocolli

Esistono vari modi per connettere una stampante al sistema. Nel caso del sistema di stampa CUPS, ai fini della configurazione, non fa differenza se la stampante è collegata in locale o tramite la rete al sistema. Sotto Linux stampanti locali vanno connesse come descritto dal produttore nelle istruzioni accluse. CUPS supporta le seguenti tipologie di connessione: "seriale", "USB", "parallela" e "SCSI". Per connettere la stampante consultate anche gli articoli della nostra banca dati di supporto sotto: `http://portal.suse.com`, eseguendo una ricerca utilizzando la parola chiave *cups*, tra cui segnaliamo *CUPS in a Nutshell*

Avvertimento

Connessione via cavo al sistema

Quando connettete la stampante al sistema con un cavo dovete tenere presente che solo nel caso di connessioni USB è possibile effettuare la connessione o disconessione con il sistema in esecuzione. Tutti gli altri tipi di connessione vanno effettuate a sistema spento.

Avvertimento

12.4 Installazione del software

"PostScript Printer Description" (PPD) descrive le caratteristiche (ad es. risoluzione) e opzioni possibili (ad es. unità duplex) della stampante. Questa descrizione permette di utilizzare sotto CUPS le diverse opzioni offerte dalla stampante. Senza file PPD, i dati da stampare vengono passati alla stampante in uno stato "grezzo", cosa in genere non desiderabile. SUSE LINUX fornisce a corredo una serie di file PPD preinstallati per poter appunto utilizzare anche stampanti che non supportano PostScript.

Se si dispone di una stampante PostScript, si consiglia di reperire il file PPD adatto. Molti file PPD sono contenuti nel pacchetto `manufacturer-PPDs` che viene installato automaticamente durante l'installazione standard; cfr. la sezione 12.7.4 a pagina 264 e la sezione 12.8.2 a pagina 267.

Dei nuovi file PPD vanno archiviati nella directory `/usr/share/cups/model/` o meglio ancora vanno aggiunti al sistema di stampa tramite YaST si veda la sezione Configurazione manuale nella pagina successiva. In tal modo si potrà ricorrere a questo tipo di file in modo preferenziale durante il processo di installazione.

Cauti bisogna essere in quei casi in cui il produttore della stampante vi chiede di modificare dei file di configurazione e di installare inoltre degli interi pacchetti software. Tenete presente che una volta installato dei pacchetti del genere non potrete più usufruire del servizio di supporto elargito da SUSE LINUX ed inoltre non stupitevi se dei comandi di stampa non dovessero produrre il solito effetto, e se il sistema non dovesse essere più in grado di indirizzare dei dispositivi di altri produttori. Quindi, in linea di massima si sconsiglia di installare del software specifico di un produttore.

12.5 Configurazione della stampante

Una volta connessa la stampante al computer ed installato il software, si passa alla configurazione della stampante. Si consiglia di utilizzare a riguardo esclusivamente gli strumenti forniti a corredo da SUSE LINUX. Visto che in SUSE LINUX la sicurezza ha priorità assoluta, strumenti di terzi spesso incontrano delle difficoltà nel maneggiare le limitazioni imposte per motivi di sicurezza e così alla fine più che un aiuto o rimedio questi strumenti alla fine si rivelano essere piuttosto la causa di difficoltà.

12.5.1 Stampanti locali

Se al login viene rilevata una stampante non ancora configurata si avvia un modulo YaST per procedere alla sua configurazione.

Per configurare la stampante dovete selezionare nel centro di controllo di YaST 'Hardware' → 'Stampante'. Comparirà la finestra principale per la configurazione della stampante. In alto avete le stampanti rilevate, in basso le code di stampa sin qui configurate. Se una stampante non viene rilevata automaticamente, potete configurarla manualmente.

Importante

Se la voce 'Stampante' non è disponibile nel centro di controllo di YaST, molto probabilmente il pacchetto `yast2-printer` non è stato installato. Per risolvere il problema installate il pacchetto `yast2-printer` e riavviate YaST.

Importante

Configurazione automatica

YaST vi permette di configurare in modo automatico una stampante, se la porta parallela o la porta USB si lascia impostare automaticamente e se la stampante connessa ad essa è stata rilevata. Nella banca dati delle stampanti vi è l'ID del modello della stampante, che YaST ha rilevato durante il processo di rilevamento hardware automatico. Questo ID hardware a volte nel caso di alcune stampanti differisce dalla denominazione del modello. In questi casi il modello va selezionato manualmente.

Per ogni tipo di configurazione si dovrebbe eseguire un test di stampa per verificare il corretto funzionamento del processo di stampa. Il risultato del test fornisce inoltre ulteriori informazioni importanti relative alla configurazione sottoposta al test.

Configurazione manuale

Se uno dei presupposti per la configurazione automatica non è dato o si desidera eseguire una configurazione particolare, personalizzata allora la configurazione deve essere realizzata manualmente. A seconda dell'estensione del rilevamento automatico effettuato da YaST e in base alle informazioni disponibili nella banca dati delle stampanti relative al modello in questione, YaST è in grado di proporre una preselezione sensata.

Ecco i valori che vanno impostati:

Connessione hardware (porta) La configurazione della connessione hardware dipende dal fatto se YaST ha potuto rilevare la stampante durante il processo di rilevamento hardware. In caso affermativo, si può partire dal presupposto che la connessione della stampante a livello hardware funziona e non vi è alcuna necessità di intervenire. In caso negativo, cioé YaST non rileva il modello della stampante, la connessione della stampante a livello hardware va configurata manualmente.

Nome della coda di stampa Considerato il fatto che il nome della coda di stampa va indicato ogni volta che si vuole stampare qualcosa, si consiglia di scegliere una nome breve composto da minuscole ed eventualmente da cifre.

Modello di stampante e file PPD Le impostazioni specifiche di una stampante (ad es. driver Ghostscript e relativi parametri del filtro di stampa per il driver) si trovano in un file PPD (ingl. PostScript Printer Description); in tema di file PPD si veda la sezione 12.4 a pagina 253.

Molte stampanti dispongono di diversi file PPD (ad es. se per un dato modello vanno bene diversi driver Ghostscript). Selezionando il produttore e il modello si selezionano in un primo tempo solo i file PPD appropriati per la stampante. Se sono disponibili diversi file PPD, YaST seleziona tra questi un file PPD (di solito quello caratterizzato dalla voce recommended, ovvero raccomandato o consigliato). All'occorrenza potete selezionare un altro file PPD premendo 'Modifica'.

Nel caso di stampanti non PostScript i dati destinati alla stampante vengono generati dal driver Ghostscript. Per tal ragione è determinante la configurazione del driver Ghostscript per ottenere dei risultati di qualità per quel che riguarda le stampe. Il driver Ghostscript scelto (tramite file PPD) e le rispettive impostazioni riguardanti il driver determineranno il risultato del processo di stampa. All'occorrenza sussiste la possibilità di selezionare nel file PPD impostazioni driver diverse da applicare tramite 'Modifica'.

Si consiglia caldamente di eseguire un test di stampa con YaST. Se il test produce dei risultati inattesi (ad es. tanti fogli quasi vuoti), potete fermare il processo di stampa rimuovendo tutti i fogli e interrompere quindi il test.

Se il modello della stampante non è incluso nella banca dati delle stampanti potete aggiungere un nuovo file PPD selezionando 'Aggiungi file PPD alla banca dati' o scegliere tra una serie di file PPD generici per i linguaggi di stampa standard. Selezionate a riguardo 'UNKNOWN MANUFACTURER', ovvero produttore sconosciuto quale "Produttore".

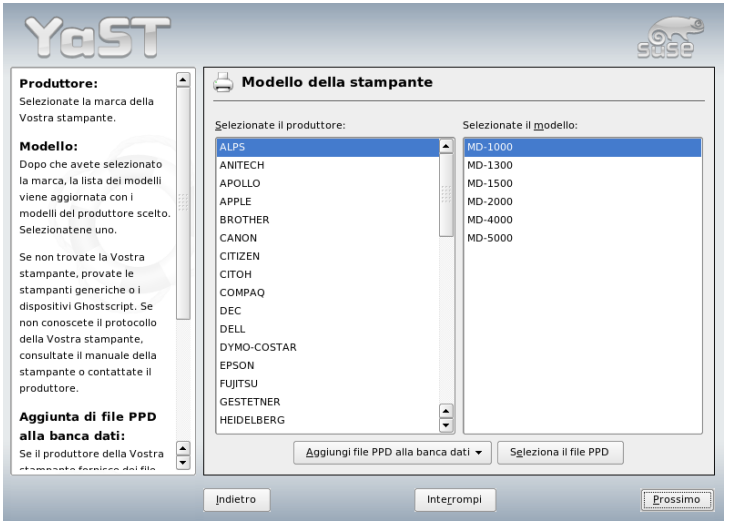

Figura 12.1: *Selezione del modello della stampante*

Impostazioni avanzate Di solito non sarà necessario modificare queste impostazioni.

Configurare la stampante tramite dei tool da linea di comando

Per configurare la stampante manualmente ricorrendo a degli strumenti da linea di comando (si veda la sezione Configurazione tramite tool a linea di comando a pagina 258) è richiesta un URI (ingl. uniform resource identifier) del dispositivo composta dal back-end, ad es. USB, e dei parametri, tipo /dev/usb/lp1. Ad esempio, un URI completo potrebbe assumere il seguente aspetto `parallel:/dev/lp0` (stampante connessa alla prima porta parallela) o `usb:/dev/usb/lp0` (prima stampante rilevata connessa alla porta USB).

12.5.2 Stampante di rete

Una stampante di rete supporta diversi protocolli e alcuni addirittura simultaneamente. La maggioranza dei protocolli supportati sono standardizzati, comunque

può darsi il caso che il produttore estenda lo standard o lo modifichi dopo averlo sottoposto a dei test su sistemi che non hanno implementato lo standard in modo corretto oppure perché desidera implementare determinate funzionalità non previste dallo standard. Driver del genere sono spesso disponibili solo per pochi sistemi operativi tra cui purtroppo solo in casi rari figura anche Linux. Attualmente non si può partire dal presupposto che ogni protocollo armonizzi bene con Linux e quindi si dovrà sperimentare un pò prima di giungere ad una configurazione funzionante a tutti gli effetti.

CUPS supporta i protocolli `socket`, `LPD`, `IPP` e `smb`. Riportiamo di seguito alcune informazioni dettagliate riguardanti questi protocolli:

socket *socket* indica una connessione nella quale i dati vengono inviati tramite un cosiddetto Internet socket senza che vi sia stato in precedenza un'operazione di handshake dei dati. I numeri di porta per connessioni socket tipici sono `9100` oppure `35`. Segue un esempio per l'URI di un dispositivo: `socket://host-printer:9100/`

LPD (Line Printer Daemon) Il protocollo LPD è un protocollo già collaudato nel tempo. LPD sta per "Line Printer Daemon" e viene descritto nell'RFC 1179. Questo protocollo si distingue per il fatto che prima di inviare i dati effettivi da stampare, spedisce i dati relativi all'incarico, ad esempio la coda di stampa. Quindi è necessario indicare una coda di stampa durante il processo di configurazione del protocollo LPD ai fini della trasmissione dei dati. Le implementazioni delle varie case produttrici sono così tolleranti che accettano un nome qualsiasi per la coda di stampa. Altrimenti il nome da utilizzare effettivamente è reperibile nella documentazione della stampante. Spesso si ha LPT, LPT1, LP1 o nomi simili. Chiaramente, con CUPS è possibile configurare una coda LPD di un altro sistema Linux o Unix-like. Il numero di porta per il servizio LPD è `515`. Ecco un esempio per un URI di dispositivo: `lpd://host-printer/LPT1`

IPP (Internet Printing Protocol) L'Internet Printing Protocol, abbreviato con IPP, è un protocollo relativamente recente (dell'anno 1999) che si basa sul protocollo HTTP. IPP invia un numero considerevolmente maggiore di dati relativi ad un incarico rispetto ad altri protocolli. CUPS utilizza IPP la trasmissione interna dei dati. Se intendete impostare una coda di inoltro (ingl. forwarding queue) tra due server CUPS, date la preferenza ad IPP. Anche in questo caso è richiesto il nome della coda di stampa per una corretta configurazione dell' IPP. Il numero di porta per IPP è `631`. Esempio per un URI del dispositivo: `ipp://host-printer/ps` o: `ipp://host-cupsserver/printers/ps`

SMB (share Windows) Infine CUPS premette di stampare da una share Windows. Il protocollo del caso si chiama SMB ed i numeri di porta sono `137`, `138` e `139`. Esempio per un URI di dispositivo `smb://user:password@workgroup/server/printer` o: `smb://user:password@host/printer` o: `smb://server/printer`

Prima di iniziare con la configurazione va stabilito il protocollo supportato dalla stampante. Se il produttore non dà delle indicazioni a riguardo, grazie al comando `nmap` (pacchetto `nmap`) è possibile determinarlo. `nmap` rivela le porte attivate di un host; per esempio:

```
nmap -p 35,137-139,515,631,9100-10000 printerIP
```

12.5.3 Il processo di configurazione

Potete eseguire la configurazione tramite YaST o tramite tool a riga di comando.

Configurare CUPS nella rete con YaST

Stampanti di rete dovrebbero essere configurate ricorrendo a YaST che semplifica il processo configurativo ed offre inoltre tutti gli strumenti per gestire le restrizioni di sicurezza di CUPS (si veda la sezione 12.7.2 a pagina 262).

Per delle linee guida in tema di installazione di CUPS in una rete consultate l'articolo della nostra banca di dati di supporto *CUPS in a Nutshell* che trovate al seguente indirizzo `http://portal.suse.com`.

Configurazione tramite tool a linea di comando

Alternativamente sussiste la possibilità di configurare CUPS tramite tool a linea di comando come `lpadmin` e `lpoptions`. Creati i presupposti (il file PPD è noto come anche l'URI del dispositivo), basta eseguire le seguenti operazioni:

```
lpadmin -p coda -v URI-del-dispositivo \
-P PPD-file -E
```

L'importante è che `-E` non sia la prima opzione, dato che con tutti i comandi CUPS `-E` quale primo argomento indica che si desidera ricorrere ad una connessione cifrata (ingl. encrypted) e non di abilitare la stampante come è invece l'intento dell'esempio riportato sopra (ingl. enable). Un esempio concreto:

```
lpadmin -p ps -v parallel:/dev/lp0 \
  -P /usr/share/cups/model/Postscript.ppd.gz -E
```

Esempio analogo per una stampante di rete:

```
lpadmin -p ps -v socket://192.168.1.0:9100/ -P \
/usr/share/cups/model/Postscript-level1.ppd.gz -E
```

Modificare delle opzioni

Durante il processo di installazione del sistema alcune opzioni vengono impostate di default. Le opzioni possono essere modificate con ogni incarico di stampa (in base al tool di stampa utilizzato); vi è comunque anche la possibilità di modificare le opzioni di default ricorrendo a YaST. Ecco come procedere in tal caso utilizzando dei tool a linea di comando:

1. Innanzitutto elencate le opzioni:

   ```
   lpoptions -p coda_di_stampa -l
   ```

   Esempio:

   ```
   Resolution/Output Resolution: 150dpi *300dpi 600dpi
   ```

   Un'opzione abilitata di default si riconosce dall'asterisco (`*`) che la precede `*`

2. Intervenite sull' opzione tramite `lpadmin`:

   ```
   lpadmin -p queue -o Resolution=600dpi
   ```

3. Controllate che tutto sia andato per il verso giusto:

   ```
   lpoptions -p queue -l

   Resolution/Output Resolution: 150dpi 300dpi *600dpi
   ```

12.6 Configurazione per gli applicativi

Gli applicativi ricorrono alle code di stampa configurate, analogamente al processo di stampa dalla linea di comando. Quindi di solito non bisogna configurare nuovamente la stampante per un dato applicativo ma basterà utilizzare le code di stampa esistenti.

12.6.1 Stampare dalla linea di comando

Per stampare dalla linea di comando, immettete il comando `lp -d` ⟨*`nomecodadistampa`*⟩ ⟨*`nomefile`*⟩, specificate i nomi del caso per ⟨*nomecodadistampa*⟩ e ⟨*nomefile*⟩.

12.6.2 Stampare da un applicativo utilizzando un tool a linea di comando

Alcune applicazioni utilizzano il comando `lp` per stampare. In tal caso, immettete il comando corretto nella finestra dialogo dell'applicazione (ma solitamente senza specificare ⟨*nomefile*⟩), ad esempio, `lp -d` ⟨*`nomecodadistampa`*⟩. Nel caso di applicativi KDE dovete abilitare la voce 'Stampare tramite un programma esterno', altrimenti non sarà possibile immettere ed eseguire alcun comando di stampa.

12.6.3 Utilizzare il sistema di stampa CUPS

Strumenti di lavoro tipo xpp o il programma KDE kprinter dispongono di un'interfaccia grafica che consente all'utente di selezionare la coda di stampa e di impostare le opzioni di default per CUPS nonché opzioni specifiche della stampante tra quelle previste nel file PPD. Potete utilizzare kprinter quale interfaccia di stampa di default anche per applicazioni non KDE specificando `kprinter` o `kprinter --stdin` quale comando di stampa nelle finestre dialogo di stampa delle relative applicazioni. Il comando di stampa è da scegliere in base all'applicativo. Se le impostazioni sono state eseguite correttamente, l'applicativo richiamerà la finestra dialogo di stampa di kprinter ogni volta che si intende eseguire un incarico di stampa, dandovi così il modo di selezionare la coda di stampa e di effettuare le impostazioni del caso. Per seguire questo approccio dovete assicurare che le impostazioni di stampa della applicazione non siano in conflitto con quelle di kprinter. Si consiglia di modificare le impostazioni di stampa solo tramite kprinter, dopo averlo abilitato.

12.7 Particolarità di SUSE LINUX

Alcune funzionalità di CUPS sono state rivisitate per permetterne l'esecuzione su SUSE LINUX. Segue una breve rassegna delle modifiche di maggior rilevanza apportate.

12.7.1 Server CUPS e firewall

Vi sono svariati modi di configurare CUPS come client di un server di rete.

- Per ogni coda di stampa gestita dal server di rete, si può impostare una coda di stampa locale tramite la quale inoltrare tutti gli incarichi di stampa al rispettivo server di rete. Questo approccio è sconsigliato per il fatto che ogni modifica apportata alla configurazione del server di rete comporta dover riconfigurare tutti i client.
- Si potranno anche inoltrare gli incarichi di stampa direttamente ad un server di rete. Per una configurazione del genere non è necessario che vi sia un demone CUPS in esecuzione. `lp` (o le corrispondenti chiamate di libreria di altri programmi) possono inviare gli incarichi direttamente al server di rete. Una configurazione del genere però non funziona se si vuole stampare anche tramite una stampante connessa localmente.
- Il daemon CUPS capta pacchetti IPP inviati da altri server di rete per annunciare le code di stampa disponibili. Si tratta della miglior configurazione CUPS possibile - se si vuole stampare tramite server CUPS remoti. Questo assetto configurativo è comunque esposto al rischio di incappare in una coda di stampa contraffatta di un aggressore, senza che l'utente se ne accorga in un primo momento. Se si vuole ricorrere comunque a questo metodo, la porta 631/UDP deve accettare pacchetti in entrata.

YaST conosce due modi per rilevare server CUPS nella rete: scandire la rete (ingl. "scan") per rilevare se degli host sulla rete offrono questo servizio mettendosi in ascolto di broadcast IPP. Il secondo metodo viene applicato già durante il processo di installazione quando YaST cerca di rilevare dei server CUPS da includere nel suo elenco proposta. Anche in questo caso la porta 631/UDP deve accettare pacchetti in entrata.

In tema di firewall va aggiunto quanto segue: l'impostazione di default del firewall proposta è quella di *non* accettare alcun broadcast IPP. Ciò vuol dire che il secondo metodo per rilevare delle code di stampa remote ed il terzo metodo per indirizzare code remote non funzionano. Quindi va modificata la configurazione del firewall: o si contrassegna una delle interfacce come `internal`, ossia interna e in tal modo la porta viene aperta di default o si apre in modo mirato la porta di un'interfaccia esterna (`external`); per motivi di sicurezza tutte le porte devono essere chiuse di default. Anche l'apertura esclusivamente ai fini di rilevamento (per indirizzare code remote in base al metodo 2) rappresenta un rischio

in termini di sicurezza, dato che gli utenti possano incappare in un server di un aggressore.

Riassumendo: l'utente deve modificare la configurazione del firewall proposta per poter consentire a CUPS di rilevare code di stampa remote durante il processo di installazione ('Apri porta nel firewall') e per poter in seguito nel modo operativo normale indirizzare i vari server remoti dal sistema locale. Un'alternativa: l'utente dà l'incarico al sistema di rilevare il server CUPS scandendo (ingl. scan) i sistemi presenti sulla rete locale o configura manualmente tutte le code di stampa (cosa che per i motivi sopramenzionati non è consigliata).

12.7.2 Amministrare CUPS tramite web frontend

Per poter eseguire l'amministrazione tramite il web frontend (CUPS) o tramite lo strumento di amministrazione della stampante (KDE) va creato l'utente `root` quale amministratore CUPS del gruppo di amministrazione CUPS `sys` corredato di una password CUPS; ciò può venir realizzato dando come `root` il seguente comando:

```
lppasswd -g sys -a root
```

Altrimenti non è possibile eseguire l'amministrazione tramite interfaccia web o strumento di amministrazione, visto che se manca l'amministratore CUPS non è possibile eseguire l'autenticazione. Al posto di `root` si può anche stabilire un altro utente come amministratore CUPS; si veda la sezione 12.7.3 in questa pagina.

12.7.3 Modifiche al servizio di stampa CUPS (cupsd)

Queste modifiche sono state applicate originariamente a SUSE LINUX 9.1.

cupsd gira come utente lp

Dopo l'avvio, `cupsd` effettua il passaggio dall'utente `root` all'utente `lp`. In tal modo aumenta il livello di sicurezza visto che il servizio di stampa CUPS non gira con permessi illimitati, ma solo con quei permessi richiesti per il servizio di stampa.

Uno svantaggio però è rappresentato dal fatto che l'autenticazione (più precisamente: la verifica del password) non avviene tramite `/etc/shadow` dato che `lp`

non ha accesso a /etc/shadow. Invece si deve ricorrere all'autenticazione specifica di CUPS tramite /etc/cups/passwd.md5. A tal fine va inserito l'amministratore CUPS, il gruppo di amministrazione CUPS sys ed una password CUPS in /etc/cups/passwd.md5; immettete come root:

```
lppasswd -g sys -a CUPS-admin-name
```

Se cupsd gira come lp, non si può generare /etc/printcap per il fatto che lp non ha il permesso di generare dei file in /etc/. Per questo motivo cupsd genera /etc/cups/printcap ed affinché sia garantito il corretto funzionamento delle applicazioni che leggono i nomi delle code di stampa solo da /etc/printcap, vi è un link simbolico che punta su /etc/cups/printcap.

Non appena cupsd gira come lp non è più possibile accedere alla porta 631 e così non è più possibile eseguire un reload di cups tramite un rccups reload. Ricorrete invece a rccups restart.

Funzionalità generalizzate per BrowseAllow e BrowseDeny

I permessi di accesso stabilite con BrowseAllow e BrowseDeny valgono per ogni tipo di pacchetto inviato a cupsd. Le impostazioni di default in /etc/cups/cupsd.conf sono:

```
BrowseAllow @LOCAL
BrowseDeny All
```

e

```
<Location />
  Order Deny,Allow
  Deny From All
  Allow From 127.0.0.1
  Allow From 127.0.0.2
  Allow From @LOCAL
</Location>
```

In tal modo solo i sistemi LOCAL accedono al cupsd in esecuzione sul server CUPS. I sistemi LOCAL sono quelli con un indirizzo IP appartenente ad una interfaccia cosiddetta non-PPP (point-to-point), più precisamente: interfacce senza un flag IFF_POINTOPOINT impostato) e il cui indirizzo IP appartiene alla stessa rete del server CUPS. Pacchetti provenienti da altri host vengono subito rifiutati.

Attivazione di default di cupsd

Nel corso di una installazione standard `cupsd` viene abilitato automaticamente. Questo consente di accedere comodamente, senza dover intervenire manualmente, a code di stampa dei server di rete CUPS. Le prime due voci (si veda la sezione cupsd gira come utente lp a pagina 262 e sezione Funzionalità generalizzate per BrowseAllow e BrowseDeny nella pagina precedente) sono delle condizioni necessarie per realizzare una attivazione automatica di `cupsd` in tutta sicurezza.

12.7.4 File PPD nei diversi pacchetti

Configurazione della stampante solo tramite file PPD

Durante il processo configurativo della stampante effettuato tramite YaST vengono impostate le code di stampa per CUPS ricorrendo esclusivamente ai file PPD installati sotto `/usr/share/cups/model/` del sistema. YaST individua i file PPD adatti per una determinata stampante comparando il nome del modello ed il nome del produttore, rilevati durante il processo di riconoscimento hardware, con quelli del produttore e del modello dei file PPD dei rispettivi sistemi reperibili sotto `/usr/share/cups/model/`. A tal fine, durante il processo di configurazione della stampante eseguito con YaST, viene generata una banca dati composta da informazioni, presi dai file PPD, riguardanti il produttore ed il modello in questione. In questo modo vi è possibile selezionare la vostra stampante tramite il nome del modello e del produttore e ottenere dei file PPD adatti al modello in questione.

Eseguire la configurazione avvalendosi esclusivamente dei file PPD senza ricorrere ad ulteriori fonti di informazioni comporta il vantaggio di poter modificare a piacimento i file PPD residenti in `/usr/share/cups/model/`. Il rispettivo modulo di YaST riconosce le modifiche apportate e genera una nuova banca dati composta dai dati riguardanti casa produttrice e modello della stampante. Se ad esempio disponete solo di stampanti PostScript solitamente non dovete ricorrere né ai file PPD Foomatic reperibili nel pacchetto `cups-drivers` né ai file PPD GimpPrint che trovate nel pacchetto `cups-drivers-stp`, ma solo copiare i file PPD tagliati per le vostre stampanti PostScript sotto `/usr/share/cups/model/` (se non sono già inclusi nel pacchetto `manufacturer-PPDs`) al fine di configurare la vostra stampante in modo corretto.

File PPD CUPS nel pacchetto cups

I file PPD generici del pacchetto `cups` sono stati integrati con i seguenti file PPD Foomatic appropriati per stampanti PostScript level 2 e level 1:

- /usr/share/cups/model/Postscript-level1.ppd.gz
- /usr/share/cups/model/Postscript-level2.ppd.gz

File PPD Foomatic nel pacchetto cups-drivers

Per stampanti non PostScript di solito si ricorre al filtro di stampa Foomatic foomatic-rip affiancato a Ghostscript. I file PPD appropriati Foomatic sono contraddistinti da "*NickName: ... Foomatic/Ghostscript driver e *cupsFilter: ... foomatic-rip. Questi file PPD si trovano nel pacchetto cups-drivers.

YaST dà la preferenza ad un file PPD Foomatic se vi è un file PPD Foomatic con la voce *NickName: ... Foomatic ... (recommended) adatto al modello della stampante, e nel pacchetto manufacturer-PPDs non vi è alcun file PPD più adatto (si veda sotto).

File PPD GimpPrint nel pacchetto cups-drivers-stp

Molte stampanti non PostScript consentono utilizzo del filtro CUPS rastertoprinter di GimpPrint al posto di foomatic-rip. Questo filtro e i file PPD GimpPrint sono reperibili nel pacchetto cups-drivers-stp. I file PPD GimpPrint si trovano sotto /usr/share/cups/model/stp/ e sono contraddistinti da *NickName: ... CUPS+Gimp-Print e *cupsFilter: ... rastertoprinter.

File PPD dei produttori nel pacchetto manufacturer-PPDs

Il pacchetto manufacturer-PPDs contiene dei file PPD messi a disposizione dalle case produttrici coperti da una licenza gratuita. Stampanti PostScript dovrebbero essere configurate ricorrendo al file PPD appropriato del produttore, visto che il file PPD del produttore consente di sfruttare tutte le funzionalità della stampante PostScript. YaST preferisce utilizzare un file PPD preso dai manufacturer-PPDs, se sono date le seguenti condizioni:

- Il nome del modello e del produttore rilevati durante il riconoscimento hardware sono identici a quelli contenuti nel file PPD del pacchetto manufacturer-PPDs.
- Il file PPD del pacchetto manufacturer-PPDs è l'unico ad essere adatto al modello della stampante o vi è anche un file PPD Foomatic adatto che reca la seguente dicitura *NickName: ... Foomatic/Postscript (recommended).

Nei casi riportati di seguito YaST non ricorre a dei file PPD presi da `manufacturer-PPDs`:

- Il file PPD del pacchetto `manufacturer-PPDs` non collima per quel che riguarda il nome della casa produttrice e nome del modello. Cosa che si verifica spesso se il pacchetto `manufacturer-PPDs` presenta solo un file PPD per modelli simili (ad es. nel caso in cui per la serie di un modello non è stato generato un file PPD per ogni modello della serie e come nome del modello nel file PPD vi è una indicazione del tipo `Serie Funprinter 1000`).
- Il file PDD Postscript Foomatic non è del tipo "recommended", per motivi dovuti al fatto che ad esempio il modello della stampante non funziona bene nel modo PostScript, ovvero è inaffidabile perché la stampante dispone di insufficente memoria oppure di un processore troppo lento, oppure infine perché non supporta PostScript di default (ad es. perché il supporto a PostScript è disponibile solo sotto forma di modulo opzionale).

Se per una stampante PostScript vi è un file PPD appropriato in `manufacturer-PPDs` ma YaST, per i motivi sopracitati non è in grado di gestirlo, allora il modello di stampante adatto va selezionato manualmente.

12.8 Possibili difficoltà e la loro risoluzione

Nelle seguenti sezioni descriveremo le difficoltà relative all'hardware e al software che si possono verificare durante il processo di stampa ed il modo di risolverli.

12.8.1 Stampanti sprovviste di un linguaggio standard

Una stampante che può essere indirizzata solo attraverso delle particolari sequenze di controllo si chiamano *stampanti GDI*. Questo tipo di stampante funziona solo con la versione di un sistema operativo per la quale il produttore acclude i driver. *GDI* è una interfaccia di programmazione sviluppata dalla Microsoft per dispositivi grafici. Il problema non è rappresentato dalla interfaccia ma piuttosto dal fatto che le cosiddette stampanti GDI possono essere indirizzate *esclusivamente* per via di un linguaggio di stampante proprietario.

Esistono delle stampanti che oltre al modo GDI comprendono anche un linguaggio standard e basta impostarle di conseguenza, oppure che permettono di passare da un modo all'altro. Per alcune stampanti GDI vi sono dei driver proprietari forniti dalla casa produttrice. Lo svantaggio di tali driver è che non si può garantire che armonizzino bene con il sistema di stampa installato né che lo facciano indistintamente con tutte piattaforme hardware. Le stampanti che invece supportano un linguaggio standard non dipendono né da una versione in particolare del sistema di stampa né da una determinata piattaforma hardware.

Di solito non vale la pena investire del tempo nel tentativo di adattare un driver Linux proprietario, conviene piuttosto acquistare direttamente una stampante supportata. Non vale la pena in primo luogo perché con una stampante che funziona in modo ineccepibile il problema dei driver viene risolto una volta per tutte. Inoltre non è più necessario installare ed eventualmente configurare del software driver particolare ed infine non si dovrà andare a cercare gli aggiornamenti del driver nel caso in cui il sistema di stampa è stato modificato nelle versioni successive.

12.8.2 Manca file PPD adatto per stampante PostScript

Se nel pacchetto manufacturer-PPDs non si trova alcun file PPD adatto ad una stampante PostScript dovrebbe essere comunque possibile utilizzare un file PPD reperibile sul CD dei driver del produttore o scaricare un file PPD adatto dal sito web della casa produttrice della stampante.

Se il file PPD si presenta sotto forma di archivio zip (estensione .zip) oppure sotto forma di archivio zip auto scompattante (`.exe`) potete utilizzare `unzip` per scompattarlo. Informatevi innanzitutto sui termini licenza del file PPD. Eseguite quindi un test con l'utility `cupstestppd` per vedere se il file PPD si attiene alla "Adobe PostScript Printer Description File Format Specification, Version 4.3". Se viene visualizzato "FAIL" vuol dire che vi sono degli errori gravi nel file PPD e fate conto che soregeranno delle grosse difficoltà. Cercate di risolvere i problemi rilevati da `cupstestppd`. Se necessario rivolgetevi direttamente al produttore per richiedere un file PPD che faccia al vostro caso.

12.8.3 Porte parallele

Il miglior approccio consiste nel connettere la stampante direttamente alla prima interfaccia parallela, e selezionare nel BIOS le seguenti impostazioni per l'interfaccia parallela:

- Indirizzo IO `378` (esadecimale)
- L'interrupt: irrelevante
- Modo: `Normal`, `SPP` oppure `Output Only`
- DMA: disabled

Se nonostante queste impostazioni del BIOS la stampante non risulta essere indirizzabile tramite la prima porta parallela, l'indirizzo IO - seguendo l'impostazione del BIOS - va inserito esplicitamente con `0x378` in `/etc/modprobe.conf`. Se vi sono due porte parallele impostate sugli indirizzi IO `378` e `278` (esadecimale), allora essi vanno inseriti nel seguente modo `0x378,0x278`.

Se l'interrupt `7` non è stato ancora assegnato, potete farlo prendendo spunto dall'esempio 12.1 in questa pagina. Prima di abilitare l'interrupt date una occhiata al file `/proc/interrupts` per vedere quali interrupt vengono già usati; comunque dovete considerare che vengono indicati solo gli interrupt utilizzati in quel momento, condizione che mutua in base ai componenti hardware attivamente utilizzati. Tenete presente che l'interrupt per la porta parallela non può venir già utilizzato da qualche dispositivo del sistema. In caso di dubbio impostate il modo polling con `irq=none`.

Esempio 12.1: */etc/modprobe.conf: l'interrupt per la prima porta parallela*

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

12.8.4 Connettere la stampante di rete

Rilevare problemi dovuti alla rete Connettete la stampante direttamente ad un computer. Configurate la stampante come stampante locale ed eseguite un test di stampa; se tutto va per il verso giusto le difficoltà non possono che essere dovute alla rete.

Controllare la rete TCP/IP La rete TCP/IP deve funzionare in modo ineccepibile come anche la risoluzione dei nomi.

Controllare un `lpd` remoto Con il seguente comando potete testare se è possibile connettersi tramite TCP all' lpd (porta `515`) del sistema ⟨*host*⟩:

```
netcat -z host 515 && echo ok || echo failed
```

Se non è possibile connettersi all' `lpd` allora la causa può essere dovuta al fatto che l'`lpd` non è in esecuzione oppure vi sono dei vistosi problemi di rete.

Dando come utente `root` il seguente comando si può ottenere una rassegna dello stato (eventualmente molto dettagliata) sulla coda di stampa ⟨*queue*⟩ sull'⟨*host*⟩ (remoto), purché l'`lpd` dell'host remoto sia in esecuzione ed accetti delle richieste:

```
echo -e "\004queue" \
  | netcat -w 2 -p 722 host 515
```

Se l'lpd non risponde allora o l'`lpd` non è in esecuzione oppure vi sono dei problemi di rete. Se l'`lpd` risponde, allora si potrà chiarire il perché non è possibile stampare sulla coda di stampa `queue` dell'`host` – Nel caso di una risposta riportata nell'esempio 12.2 in questa pagina, la causa del problema è dovuta all'`lpd` remoto.

Esempio 12.2: *Messaggio di errore di* `lpd`

```
lpd: your host does not have line printer access
lpd: queue does not exist printer:
spooling disabled
printer: printing disabled
```

Verifica di un `cupsd` remoto Con il seguente comando potete verificare se vi è un server di rete CUPS sulla rete, il quale dovrebbe comunicare via broadcast ogni 30 secondi tramite la porta UDP `631` le sue code di stampa:

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

Dopo ca. 40 secondi dovrebbe venir visualizzato un output simile a quanto riportato nell'esempio 12.3 in questa pagina se vi è un server di rete CUPS che invia dei broadcast:

Esempio 12.3: *Broadcast del server di rete CUPS*

```
ipp://host.domain:631/printers/queue
```

Il seguente comando vi permette di verificare se è possibile creare una connessione TCP al `cupsd` (porta `631`) sull' ⟨*host*⟩:

netcat -z host 631 && echo ok || echo failed

In caso negativo `cupsd` non è in esecuzione oppure vi è un grave problema di rete. Il comando `lpstat -h host -l -t` ritorna una rassegna dello stato (eventualmente molto dettagliata) sulle coda di stampa sull'⟨*host*⟩, purché il `cupsd` dell'host remoto sia in esecuzione ed accetti delle richieste.

Il comando riportato vi permette di verificare se la coda di stampa ⟨*queue*⟩ di ⟨*host*⟩ accetta un incarico di stampa composto da un solo carattere di ritorno di carrello (ingl. carriage return),— cioé viene eseguito solo un test senza stampare effettivamente alcunché se non un foglio vuoto.

```
echo -en "\r" | lp -d queue -h host
```

Stampante di rete o printserver box: causa di difficoltà

A volte si verificano dei problemi dovuti allo spooler di stampa in esecuzione su un printserver box non appena si registra un numero elevato di incarichi di stampa. Visto che il problema è dovuto allo spooler di stampa del printserver box c'è ben poco da fare. Si può aggirare lo spooler di stampa indirizzando direttamente la stampante connessa al printserver box tramite socket TCP; si veda la sezione 12.5.2 a pagina 256.

In questo modo il printserver box funge solo da convertitore tra le diverse possibilità per la trasmissione dei dati (rete TCP/IP e stampante collegata in locale). A tal fine deve essere nota la rispettiva porta TCP del printserver box. Con la stampante accesa e connessa al printserver box, dopo aver acceso il printserver box, la porta TCP si lascia determinare tramite il programma `nmap` dal pacchetto `nmap`. Ad esempio `nmap` ⟨*`indirizzo_IP`*⟩ nel caso di un printserver box emette:

```
Port       State       Service
23/tcp     open        telnet
80/tcp     open        http
515/tcp    open        printer
631/tcp    open        cups
9100/tcp   open        jetdirect
```

L'output indica che la stampante connessa al printserver box è indirizzabile tramite socket TCP sulla porta `9100`. Di default `nmap` esegue una verifica solamente di un determinato elenco di porte generalmente note riportate in `/usr/share/nmap/nmap-services`. Per eseguire una verifica di tutte le porte possibili utilizzate il comando:

```
nmap -p <da_porta>-<a_porta> <indirizzo_IP>
```

per maggiori dettagli consultate anche la pagina di manuale di `nmap`.

Con un comando del tipo

```
echo -en "\rHello\r\f" | netcat -w 1 indirizzo-IP porta
cat file | netcat -w 1 indirizzo-IP porta
```

è possibile inviare una sequenza di caratteri oppure dei file ad una determinata porta per verificare se la stampante è indirizzabile tramite la porta specificata.

12.8.5 Errori di stampa senza messaggi di errore

Per il sistema di stampa un incarico di stampa è stato portato a termine nel momento in cui il back-end di CUPS ha concluso la trasmissione dei dati destinati alla stampante. Se in seguito durante l'ulteriore elaborazione dei dati si dovesse verificare un errore (ad esempio la stampante non riesce a stampare i dati che le sono stati trasmessi), il sistema di stampa non se ne accorge neanche. Se la stampante non riesce a stampare i dati, allora si dovrebbe selezionare un altro file PPD più congruo alla stampante.

12.8.6 Code di stampa disabilitate

Se falliscono diversi tentativi di inviare dei dati alla stampante, il back-end di CUPS, ad esempio `usb` o `socket`, segnala un errore al sistema di stampa a `cupsd`. Il back-end decide quanti tentativi fare prima di dichiarare l'impossibilità della trasmissione dei dati. Visto che non ha senso continuare a tentare, la coda di stampa interessata viene disabilitata da `cupsd` (`disable`). Dopo aver risolto il problema, l'amministratore di sistema la deve riabilitare tramite `/usr/bin/enable`.

12.8.7 CUPS browsing: eliminare incarichi di stampa

Quando una server di rete CUPS segnala la propria coda di stampa ai client tramite browsing e sul client gira un `cupsd` adatto, allora il `cupsd` del client accetta gli incarichi di stampa degli applicativi e li inoltra subito al `cupsd` del server. Quando il `cupsd` accetta un incarico di stampa, all'incarico viene assegnato un numero di incarico. Quindi il numero dell'incarico sul client è diverso da

quello sul server. Dato che un incarico di stampa viene subito inoltrato, di solito non può venir cancellato ricorrendo al numero di incarico del client, dato che per il `cupsd` del client l'incarico di stampa si conclude con l'inoltro al `cupsd` del server.

Per cancellare l'incarico di stampa sul server utilizzate il comando `lpstat -h print-server -o` per determinare il numero di incarico sul server, sempre che il server non abbia ancora espletato interamente l'incarico di stampa, vale a dire lo abbia inviato alla stampante. Utilizzando il numero d'incarico, l'incarico sul server può essere cancellato:

```
cancel -h print-server queue-jobnumber
```

12.8.8 Incarichi di stampa con errori o transfer di dati disturbato

Gli incarichi di stampa permangono nelle code di stampa e il processo di stampa riprende se spegnete e riaccendete la stampante o se spegnete e riavviate il sistema durante il processo di stampa. Un incarico di stampa recante degli errori va cancellato dalla coda di stampa con il comando `cancel`.

Se un incarico presenta degli errori oppure il processo di comunicazione tra il sistema e la stampante risulta essere disturbato, la stampante non saprà cosa fare con i dati inviatele. Spesso l'esito è la stampa di innumerevoli fogli con dei caratteri privi di senso. Ecco come intervenire in questi casi.

1. Per interrompere il processo di stampa nel caso di stampanti a getto di inchiostro rimuovete tutti i fogli oppure nel caso di stampanti laser aprite il vassoio della stampante. Stampanti di buona qualità hanno un pulsante per interrompere il processo di stampa

2. Visto che l'incarico di stampa viene eliminato dalla coda di stampa solo dopo essere stato inviato per intero alla stampante, spesso lo si ritroverà ancora nella coda di stampa. Con `lpstat -o` oppure `lpstat -h` ⟨*`print-server`*⟩ `-o` fatevi indicare da quale coda di stampa provengono attualmente gli incarichi di stampa, e con `cancel` ⟨*`codadistampa`*⟩`-`⟨*`numeroincarico`*⟩ oppure `cancel -h` ⟨*`print-server`*⟩ ⟨*`codadistampa`*⟩`-`⟨*`numeroincarico`*⟩ potete cancellare l'incarico.

3. Certi dati vengono trasmessi alla stampante anche se l'incarico di stampa è già stato cancellato dalla coda di stampa. Verificate se vi è ancora un processo del back-end CUPS in esecuzione relativo alla coda di stampa in questione ed in caso affermativo fermatelo. Ad esempio, tramite il comando `fuser -k /dev/lp0` potete terminare tutti i processi che accedono alla stampante o più precisamente alla porta parallela.
4. Resettate completamente la stampante staccando per un pò la spina. In seguito rimettete i fogli e riaccendete la stampante.

12.8.9 Possibili cause di difficoltà in CUPS

In caso di difficoltà incontrate col sistema di stampa CUPS si consiglia di procedere nel seguente modo:

1. Impostate il `LogLevel debug` in `/etc/cups/cupsd.conf`.
2. Fermate `cupsd`.
3. Rimuovete `/var/log/cups/error_log*` per non dover passare al setaccio file di log troppo voluminosi.
4. Avviate `cupsd`
5. Ripetete l'operazione che ha causato il problema.
6. Adesso i messaggi in `/var/log/cups/error_log*`, vi potranno tornare utili nel tentativo di individuare la causa del problema.

12.8.10 Per maggiori informazioni

Nella banca dati di supporto troverete una fonte inesauribile di soluzioni per tutta una serie di problematiche. Se incontrate delle difficoltà inerenti al processo di stampa, eseguite una ricerca degli articoli attinenti che trattano questa tematica, troverete ad esempio *Installing a Printer* e *Printer Configuration from SUSE LINUX 9.2*, utilizzando "printer" come parola chiave.

13

Lavorare in tutta mobilità con Linux

Questo capitolo è incentrato sui diversi aspetti dell'impiego produttivo di dispositivi portatili con Linux. Verranno presentati brevemente i diversi campi di applicazione ed illustrate le rispettive soluzioni hardware e software. Il capitolo si chiude indicando le principali fonti di informazione che trattano questa tematica.

Con lavoro mobile i più associano computer portatili, PDA e cellulari e le varie possibilità di comunicazione che sussistono tra questi dispositivi. Nel presente capitolo estenderemo questo concetto fino ad includere componenti hardware mobili come dischi rigidi esterni o altri dispositivi di memorizzazione in grado interagire con sistemi portatili e sistemi desktop.

13.1 Notebook

Il corredo hardware dei notebook differisce da quello di un sistema desktop visto che nel caso dei notebook i criteri determinanti sono l'intercambiabilità, il consumo energetico, il peso e le dimensioni. I costruttori di hardware mobile hanno sviluppato lo standard PCMCIA (*Personal Computer Memory Card International Association*). Questo standard vale per schede di rete, schede di memoria, schede modem e ISDN nonché dischi rigidi esterni. In che modo viene realizzato il supporto a questo tipo di hardware sotto Linux (importante durante il processo di configurazione), quali sono i programmi a vostra disposizione per gestire PCMCIA e come individuare la causa di eventuali difficoltà in caso di messaggi di errori, viene illustrato nel capitolo 14 a pagina 285.

13.1.1 Risparmio energetico

La scelta di componenti di sistema ottimizzati da un punto di vista del consumo energetico rappresenta un fattore decisivo per far sì che i notebook possano essere impiegati anche scollegati dalla rete elettrica. Un altro fattore di uguale importanza per quel che riguarda il risparmio energetico è rappresentato dal sistema operativo. SUSE LINUX supporta diversi metodi che incidono sul consumo energetico del notebook e quindi sulla sua autonomia, ecco quelli principali:

- Abbassare la frequenza della CPU
- Spegnere l'illuminazione del display nei periodi di inattività
- Abbassare manualmente l'illuminazione del display
- Rimuovere dispositivi atti all'hotplug non utilizzati (CD-ROM USB, mouse esterno, schede PCMCIA inutilizzate, etc.)
- Spegnere il disco rigido in caso di inattività

Per degli approfondimenti in tema di power management sotto SUSE LINUX e sul modo di utilizzare il modulo di YaST dedicato al power management rimandiamo al capitolo 16 a pagina 307.

13.1.2 Integrazione in diversi ambienti operativi

Spesso il vostro notebook deve integrarsi in diversi ambienti operativi. Numerose funzionalità dipendono dall'ambiente dato, e i servizi alla base delle funzionalità devono essere riconfigurati. SUSE LINUX svolge questo compito per voi.

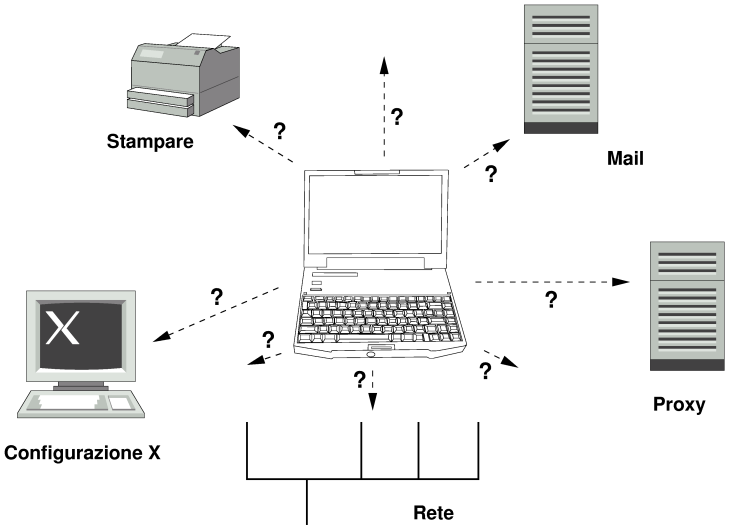

Figura 13.1: *Integrare i notebook in una rete*

I servizi in questione per notebook utilizzati sia in una propria piccola rete domestica che nella rete aziedale sono:

Configurazione di rete cioé assegnazione dell'indirizzo IP, risoluzione dei nomi e connessione a Internet o altre reti.

Stampa dovrà esistere un elenco delle stampanti disponibili e a seconda della rete ci dovrà essere anche una lista dei server di stampa disponibili.

Posta elettronica e proxy come per il caso della stampante, anche qui serve un elenco dei server da utilizzare.

Configurazione di X Se a volte connettete il vostro notebook ad un videoproiettore o a un monitor esterno dovrà essere disponibile una apposita configurazione del display.

Con SUSE LINUX avete due modi (che possono anche essere combinati) per poter integrare il vostro notebook in ambienti operativi esistenti:

SCPM SCPM (*System Configuration Profile Management*) consente di "fotografare" degli stati di configurazione del vostro sistema (detti *Profili*). I profili possono essere generati per le più disparate situazioni e sono particolarmente utili se il sistema viene utilizzato in diversi ambienti (rete domestica/rete aziendale) o se utilizzate una determinata configurazione per il vostro lavoro e un'altra per fare degli esperimenti. Potrete passare da un profilo all'altro in qualsiasi momento. Per degli approfondimenti su SCPM consultate il capitolo 15 a pagina 295. Sotto KDE potete passare da uno stato all'altro ricorrendo all'applet Kicker Profile Chooser, ovvero selezionatore dei profili. Per eseguire il programma dovete diventare root, immettendo la password di root.

SLP *Service Location Protocol* (abbrev.: SLP) semplifica la configurazione di client connessi in rete di una piccola rete locale. Per configurare il vostro notebook per un determinato ambiente di rete, in qualità di amministratore del sistema vi servono delle informazioni dettagliate sui server presenti nella rete. Tramite SLP viene indicata la disponibilità di un determinato tipo di servizio a tutti i client della rete locale. Le applicazioni che supportano SLP possono ricorrere alle informazioni distribuite tramite SLP e possono essere quindi configurate in modo automatico. SLP può essere addirittura impiegato per installare un sistema, senza dover andare alla ricerca di una fonte di installazione appropriata. Per delle informazioni dettagliate su SLP, rimandiamo al capitolo 23 a pagina 441.

SCPM è incentrato sulla generazione e il mantenimento di uno stato riproducibile del sistema, mentre SLP semplifica la configurazione automatica di un client all'interno di una rete.

13.1.3 Software e mobilità

Esistono diversi pacchetti software ideati appositamente per le diverse aree del mobile computing: per il controllo dello stato del sistema (soprattutto lo stato

di caricamento della batteria), per la sincronizzazione dei dati e per la comunicazione wireless con periferiche e Internet. Le sezioni seguenti illustrano per ogni ambito le applicazioni principali fornite a corredo con SUSE LINUX.

Controllo del sistema

In questa sezione illustreremo due tool KDE per il controllo del sistema contenuti in SUSE LINUX. Per mostrare solo lo stato della batteria del notebook vi è l'applet KPowersave contenuto in Kicker; per compiti più complessi vi è KSysguard. GNOME offre GNOME ACPI (come applet del pannello) e System Monitor per le stesse funzionalità.

KPowersave KPowersave è un applet che tramite una icona del pannello di controllo vi informa sullo stato di caricamento della batteria. L'icona indica anche il tipo di alimentazione energetica: se il dispositivo viene alimentato tramite la rete elettrica vedrete uno spinotto, se l'alimentazione è a batteria vedrete un'icona che raffigura una batteria. Tramite il relativo menu, dopo aver immesso la password di root, avviate il modulo di YaST riguardante il power management, in cui impostare il modo operativo del sistema a seconda dell'alimentazione. Per i dettagli sul power management e sul rispettivo modulo di YaST rimandiamo al capitolo 16 a pagina 307.

KSysguard KSysguard è una applicazione a sé stante, che raggruppa in una panoramica i parametri del sistema da poter monitorare. KSysguard monitora l'ACPI (stato della batteria), il carico della CPU, la rete, lo spazio libero sulle partizioni, il carico del processore e la memoria libera. Inoltre fornisce una rassegna dei processi di sistema. Il tipo di rappresentazione o filtraggio dei dati da rilevare è configurabile dall'utente. Potete tenere sott'occhio diversi parametri di sistema oppure anche parallelamente rilevare i dati di diversi host tramite la rete. KSysguard può girare anche come demone su un sistema in cui non sia stato installato l'ambiente KDE. Per maggiori informazioni su questo programma rimandiamo alla documentazione in linea del programma o al centro di assistenza SUSE.

Sincronizzazione dei dati

Se lavorate utilizzando un notebook non connesso ad una rete e una postazione di lavoro aziendale connessa in rete dovete risolvere il problema della sincronizzazione dei dati, siano essi cartelle di posta elettronica, directory o file da elaborare in azienda o durante gli spostamenti. Le possibili soluzioni per questi casi vengono illustrate nelle seguenti sezioni.

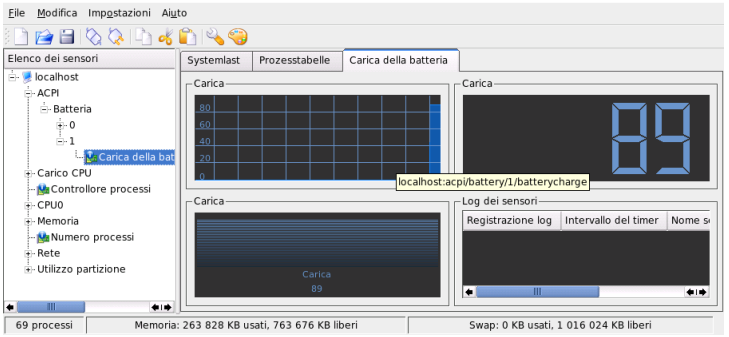

Figura 13.2: *Monitoraggio dello stato della batteria grazie a KSysguard*

Sincronizzare la posta elettronica Utilizzate un account IMAP nella rete aziendale per salvare le vostre e-mail. Sulla postazione di lavoro utilizzate un mailer qualsiasi che supporti IMAP (Mozilla Thunderbird Mail, Evolution o KMail, si veda il *Manuale dell'utente*). Su tutti i sistemi con il quale leggete la vostra posta elettronica configurate il mailer in modo che venga utilizzata sempre la stessa cartella per i `Messaggi inviati`. In tal modo tutti i messaggi sono disponibili con indicazione di stato dopo il processo di sincronizzazione. Per inviare i messaggi utilizzate il servizio SMTP del mailer al posto del MTA del sistema (postfix o sendmail) per avere informazioni attendibili sulle mail non ancora inviate.

Sincronizzazione di singoli documenti/file
Ci sono diversi programmi di utilità per sincronizzare i dati di un portatile con un PC fisso. Per informazioni dettagliate, vedete capitolo 31 a pagina 547.

Comunicazione wireless

Oltre alla comunicazione via cavo su reti domestiche o aziendali, il vostro notebook può scambiare dati anche wireless con altri sistemi, periferiche, cellulari o PDA. Linux supporta tre tipi di comunicazione wireless:

WLAN WLAN è una tecnologia wireless che permette di avere delle reti molto estese e talvolta anche dislocate. I singoli client possono essere connessi tramite WLAN a una propria rete wireless o a Internet. I cosiddetti punti

di accesso (ingl. access point) rappresentano per i client che supportano la tecnologia WLAN una sorta di stazione di base per accedere a Internet. Gli utenti di notebook con un dispositivo che supporta la tecnologia WLAN possono utilizzare diversi punti di accesso, a seconda della loro posizione e del punto di accesso che si propone loro ai fini della connessione. Come per la telefonia mobile, l'utente WLAN dispone di una grande rete senza essere legato ad una località particolare per potervi accedere. Ulteriori dettagli in tema di WLAN sono reperibili nella sezione 17.1 a pagina 334.

Bluetooth Bluetooth offre il maggior numero di possibilità di impiego tra le tecnologie wireless. Alla stregua di IrDA può essere impiegato per il processo di comunicazione tra sistema (notebook) e PDA o cellulare; può anche essere utilizzato per connettere in rete diversi client in contatto "visivo" tra loro. Inoltre Bluetooth trova applicazione nell'integrazione di componenti di sistema wireless come tastiere e mouse. Comunque non è possibile connettere in rete dispositivi dislocati. Per comunicare attraverso barriere fisiche, come le pareti di un edificio, è necessaria la tecnologia WLAN. Per maggiori informazioni su Bluetooth, i suoi campi di impiego e la sua configurazione consultate la sezione 17.2 a pagina 343.

IrDA IrDA è la tecnologia wireless con la minor portata in termini di estensione nello spazio. I dispositivi che dovranno comunicare l'uno con l'altro devono trovarsi in contatto "visivo" tra loro. Già le pareti di un edificio rappresentano una barriera insormontabile. Uno scenario di applicazione per IrDA è rappresentato dall'invio di un file dal notebook sul cellulare. Un'altra possibilità offerta da IrDA consiste ad esempio nell'invio di lavori di stampa in un ufficio. Per maggiori informazioni su IrDA rimandiamo la sezione 17.3 a pagina 354.

13.1.4 Sicurezza dei dati

La cosa migliore è proteggere i vostri dati da accessi non autorizzati in vari modi. Ecco le misure di sicurezza da considerare:

Furto Non esponete il vostro sistema al rischio di furto, tenete il vostro notebook in un luogo sicuro.

Sicurezza dei dati sul vostro sistema Non cifrate i vostri dati importanti solo durante la loro trasmissione via rete ma anche sul disco rigido. In tal modo non vengono compromessi i vostri dati neanche in caso di furto. Come

impostare una partizione cifrata sotto SUSE LINUX viene descritto nella sezione 34.3 a pagina 619.

Reti sicure Indipendentemente dal modo in cui comunicate con gli altri, il transfer dei dati proveniente dal vostro interlocutore e quello destinato ad esso dovrebbe avvenire in modo protetto. Gli aspetti generali della sicurezza sotto Linux e ambienti di rete vengono trattati nella sezione 34.4 a pagina 622. Per gli aspetti di sicurezza in ambito rete wireless si veda il capitolo 17 a pagina 333.

13.2 Hardware mobile

SUSE LINUX supporta l'integrazione automatica di dispositivi di memorizzazione mobili tramite Firewire (IEEE 1394) oppure USB. Per dispositivi di memorizzazione mobile si intendono dischi rigidi Firewire o USB, chiavi di memoria USB o macchine fotografiche digitali. Non appena questi dispositivi vengono connessi al sistema tramite le apposite interfacce, il sistema hotplug li rivela e li configura automaticamente. subfs/submount si occupa del fatto che i dispositivi vengano montati (ingl. mount) nei rispettivi punti di mount del file system. Quindi come utente non dovrete più eseguire il mount e unmount manuale dei dispositivi, come era invece necessario fare con le precedenti versioni di SUSE LINUX. Il dipositivo può essere tranquillamente rimosso non appena nessun programma vi accede.

Dischi rigidi esterni (USB e Firewire)
Non appena il sistema rileva dischi rigidi esterni, vedrete le rispettive icone sotto 'Sistema' (KDE) o 'Computer' (GNOME) nella lista dei dispositivi montati. Cliccate con il tasto sinistro del mouse sull'icona e verrà visualizzato il contenuto del dispositivo. Qui potrete creare, modificare o cancellare i file e le cartelle. Se volete identificare il disco rigido con un nome diverso da quello assegnato del sistema, fate clic con il tasto destro del mouse sull'icona per giungere al rispettivo menu contestuale e assegnate un altro nome. Questa modifica del nome si limita comunque solo a quanto visualizzato nel file manager e non influisce sul punto di mount (`/media/usb-xxx` o `/media/ieee1394-xxx`).

Chiavi di memoria USB Questi dispositivi vengono trattati dal sistema alla stregua dei dischi esterni. Potrete anche cambiarne il nome nel file manager.

Macchine fotografiche digitali (USB e Firewire)

Anche macchine fotografiche digitali rilevate dal sistema vengono visualizzate sotto forma di drive esterni nella lista del file manager. Sotto KDE potete accedere e visualizzare le immagini tramite l'URL `camera:/`. Per elaborare le immagini utilizzate digikam o gimp. Sotto GNOME, Nautilus visualizza le immagini nella rispettiva cartella file. Per amministrare e ritoccare le immagini potete usare GThumb. Per un fotoritocco più complesso il programma più completo è senz'altro Gimp. Fatta eccezione per GThumb tutti i programmi qui menzionati vengono descritti nel *Manuale dell'utente* dove trovate anche un capitolo sulle macchine fotografiche digitali.

Importante

Sicurezza dei supporti dati mobili

Proprio come i notebook anche i dischi rigidi estraibili o le chiavi di memoria sono esposti ai furti. Per evitare di compromettere i dati che si trovano su questi dispositivi si consiglia di creare una partizione cifrata come descritto nella sezione 34.3 a pagina 619.

Importante

13.3 Telefoni cellulari e PDA

Il processo di comunicazione tra un sistema desktop o un notebook e un telefono cellulare può avvenire tramite Bluetooth o IrDA. Alcuni modelli supportano entrambi i protocolli, alcuni solo uno dei due. Gli scenari di applicazione dei due protocolli e la relativa documentazione per degli approfondimenti sono stati già menzionati nella sezione Comunicazione wireless a pagina 280. La documentazione dell'apparecchio fornisce informazioni su come configurare questi protocolli sul cellulare. La configurazione lato Linux viene illustrata nelle sezione 17.2 a pagina 343 e sezione 17.3 a pagina 354.

Il supporto al processo di sincronizzazione con palmari è già integrato in Evolution e Kontact. Per l'impostazione iniziale della connessione al palmare è possibile utilizzare un procedura guidata (ingl. wizard). Conclusa questa fase iniziale, stabilite i dati da sincronizzare (indirizzi, appuntamenti, impegni e simili). Entrambi i programmi groupware vengono descritti nel *Manuale dell'utente*.

Il programma incluso in Kontact denominato KPilot è disponibile anche come programma a sé stante; una descrizione è reperible nel *Manuale dell'utente*. Vi è

inoltre il programma KitchenSync per sincronizzare dei dati riguardanti degli indirizzi.

Per maggiori informazioni su Evolution, Kontact e KPilot consultate il *Manuale dell'utente*

13.4 Ulteriori informazioni

L'indirizzo principale da consultare quanto si tratta di dispositivi mobili sotto Linux è `http://tuxmobil.org/`. In diverse sezioni vengono trattati gli aspetti concernenti l'hardware e il software di notebook, PDA, cellulari e altri componenti hardware mobili:

Un approccio simile a `http://tuxmobil.org/` viene seguito anche da `http://www.linux-on-laptops.com/` che presenta delle informazioni e notebook e palmari:

SUSE mantiene una mailing list in tedesco dedicata i notebook. Vedete `http://lists.suse.com/archive/suse-laptop/`. Su questa lista utenti e sviluppatori discutono tutti gli aspetti del mobile computing con SUSE LINUX. Le domande in inglese trovano spesso risposta ma la maggior parte del materiale archiviato è in tedesco.

In caso di difficoltà dovute al power management su notebook sotto SUSE LINUX date un'occhiate al file `README` che trovate sotto `/usr/share/doc/packages/powersave`. Questi file spesso contengono anche le impressioni o i consigli di tester e sviluppatori raccolto in extremis, spesso troverete delle indicazioni preziose per quel che riguarda la risoluzione di problemi.

PCMCIA

Questo capitolo tratta aspetti particolari dell'hardware e software PCMCIA di dispositivi portatili. PCMCIA sta per *Personal Computer Memory Card International Association* e trova applicazione come termine generale per hardware e software di questo tipo.

14.1 Hardware

La componente principale è la scheda PCMCIA, e se ne distinguono due tipi:

Schede PC sono attualmente le schede più diffuse; utilizzano un bus a 16 bit per la trasmissione dei dati e sono nella maggior parte dei casi convenienti. Alcuni recenti bridge PCMCIA hanno delle difficoltà a rilevare questo tipo di scheda, però una volta rilevata, funziona senza creare problemi.

Schede CardBus Queste schede rappresentano uno standard più recente. Viene utilizzato un bus a 32 bit e di conseguenza sono più veloci ma anche più cari. Vanno connesse al sistema alla stregua di normali schede PCI e di solito non creano delle difficoltà.

Se il servizio PCMCIA è attivo, il comando `cardctl ident` rivela il tipo di scheda inserita. Un elenco delle schede supportate si trova sotto `SUPPORTED_CARDS` in `/usr/share/doc/packages/pcmcia` con rispettivamente la versione aggiornata del PCMCIA-HOWTO.

La seconda componente necessaria è il controller PCMCIA oppure la scheda PC/bridge CardBus che crea la connessione tra la scheda e bus PCI. Vengono supportati tutti i modelli largamente diffusi. Il tipo di controller si lascia determinare tramite il comando `pcic_probe`. Se si tratta di un dispositivo PCI, il comando `lspci -vt` fornisce ulteriori informazioni.

14.2 Il software

Nella seguente sezione tratteremo gli aspetti concernenti il software PCMCIA. Descriveremo i moduli del kernel interessati e il gestore delle schede (ingl. card manager).

14.2.1 I moduli di base

I moduli del kernel richiesti risiedono nei pacchetti kernel. Sono necessari inoltre i pacchetti `pcmcia` e `hotplug`. All'avvio di PCMCIA vengono caricati i moduli `pcmcia_core`, `yenta_socket` e `ds`. Raramente al posto di `yenta_socket` è richiesto il modulo `tcic` che inizializza il controller PCMCIA e mette a disposizione le funzionalità di base.

14.2.2 Il gestore della scheda

Dato che è possibile cambiare le schede PCMCIA mentre il sistema è in esecuzione, serve un demone che controlla le attività degli slot. Questo compito viene svolto dai *CardServices* implementati nei moduli di base. L'inizializzazione della scheda inserita viene svolta dal *Gestore delle schede* (per schede PC) o sistema hotplug del kernel. Il gestore delle schede viene avviato dallo script di inizializzazione PCMCIA dopo che sono stati caricati i moduli di base; l'hotplug è automaticamente abilitato.

Se è inserita una scheda, il gestore delle schede o l'hotplug ne rivela il tipo e la funzione e carica i moduli adatti. Se i moduli sono stati caricati con successo, il gestore delle schede o l'hotplug avvia a secondo della funzione della scheda determinati script di inizializzazione che creano il collegamento di rete, montano (ingl. mount) partizioni di dischi SCSI esterni o eseguono altre operazioni in base all'hardware. Gli script del gestore delle schede si trovano in `/etc/pcmcia`. Quelli per l'hotplug in `/etc/hotplug`. Se si rimuove la scheda, il gestore delle schede o l'hotplug termina con gli stessi script le diverse attività della scheda. In seguito vengono scaricati i moduli che non occorrono più.

Processi di questo tipo vengono chiamati eventi hotplug. Se si aggiungono dei dischi rigidi o partizioni (eventi "block"), gli script hotplug ricorrono a `subfs` per fare in modo che i nuovi supporti dati siano immediatamente disponibili sotto `/media`. Per montare dei supporti dati tramite script PCMCIA meno recenti, `subfs` va disabilitato nel sistema hotplug.

Sia l'avvio di PCMCIA che gli eventi della scheda sono protocollati nel file di log del sistema (`/var/log/messages`). Lì viene registrato quale sistema PCMCIA è attualmente in uso e quale demone ha utilizzato quali script per l'impostazione.

Teoricamente una scheda PCMCIA può essere rimossa senza creare delle difficoltà. Questo funziona per schede di rete, modem o ISDN, finché non vi sono dei collegamenti di rete. Non funziona invece con partizioni montate di un disco esterno o con directory NFS. In questo caso dovete assicurarvi della sincronizzazione delle unità ed eseguire correttamente l'unmount che chiaramente non sarà più possibile una volta che avete rimossa la scheda. In caso di dubbio aiuta un `cardctleject` . Con questo comando disattivate tutte le schede del laptop. Per disattivare solo una delle schede, indicate in aggiunta il numero dello slot, p.es. `cardctl eject 0`.

14.3 La configurazione

Attraverso il runlevel editor di YaST potete determinare se avviare PCMCIA o l'hotplug al boot. Il modulo si inizializza tramite 'Sistema' → 'Editor dei runlevel'.

In `/etc/sysconfig/pcmcia` vi sono tre variabili:

`PCMCIA_PCIC` contiene il nome del modulo che gestisce il controller PCMCIA. Di solito lo script di avvio determina autonomamente il nome del modulo, se non dovesse riuscirci, potete inserire qui il modulo. Altrimenti si consiglia di non assegnare alcun valore a questa variabile.

`PCMCIA_CORE_OPTS` contiene parametri per il modulo `pcmcia_core` che comunque occorrono solo raramente. Questa opzione viene descritta nella pagina di manuale pcmcia_core(4). Visto che questa pagina di manuale si riferisce al modulo omonimo del pacchetto `pcmcia-cs` di David Hinds, essa contiene più parametri di quanto il modulo del kernel offra effettivamente, e cioè tutti quelli che iniziano con `cb_` e `pc_debug`.

`PCMCIA_BEEP` abilita e disabilita i segnali acustici del gestore delle schede.

Il gestore delle schede trova la correlazione tra driver e schede PCMCIA nei file `/etc/pcmcia/config` e `/etc/pcmcia/*.conf`. Come primo viene letto `config` e dopo `*.conf` in ordine alfabetico. L'ultima registrazione per una scheda è quella decisiva. Nella pagina di manuale di pcmcia (5) trovate i dettagli sulla sintassi di questi file.

L'allocazione dei driver e schede CardBus avviene nel file `/etc/sysconfig/hardware/hwcfg-<nomeconfigurazione>`. Questi file vengono generati da YaST durante la configurazione di una scheda. Per maggiori dettagli riguardanti la designazione della configurazione rimandiamo a `/usr/share/doc/packages/sysconfig/README` e alla pagina di manuale di getcfg (8).

14.3.1 Schede di rete

Schede di rete ethernet, wireles LAN e TokenRing si configurano come normali schede di rete con YaST. Bisogna solo selezionare come tipo di scheda `PCMCIA`. Tutti gli ulteriori dettagli sulla configurazione della rete si trovano nella sezione 22.4 a pagina 415

14.3.2 ISDN

Anche nel caso di schede da PC ISDN la configurazione avviene per sommi capi come per le altre schede ISDN se utilizzate YaST. Non importa quale delle schede ISDN venga selezionata, quello che conta è solo che si tratti di una scheda PCMCIA. Durante la configurazione dell'hardware e del provider bisogna badare che la modalità operativa sia sempre `hotplug`, e non `onboot`. Vi sono dei cosiddetti modem ISDN anche per schede PCMCIA. Si tratta di schede modem o multifunzionali con un kit di connessione ISDN che vengono trattati alla stregua di modem.

14.3.3 Modem

Con schede PC modem di solito non ci sono delle impostazioni specifiche per PCMCIA. Appena viene inserito un modem, è disponibile sotto `/dev/modem`. Anche tra le schede PCMCIA vi sono dei softmodem non supportati da Linux. Se vi sono dei driver, questi vanno integrati nel sistema.

14.3.4 SCSI ed IDE

Il modulo driver adatto viene caricato dal gestore delle schede o dall'hotplug. Non appena viene inserita una scheda SCSI o IDE, i dispositivi connessi sono a vostra disposizione. I nomi di dispositivo vengono determinati in modo dinamico. Sotto `/proc/scsi` o `/proc/ide` trovate delle informazioni su dispositivi SCSI o IDE disponibili.

Dischi rigidi esterni, lettori di CD-Rom e dispositivi simili devono essere attivati, prima di inserire la scheda PCMCIA nello slot. I dispositivi SCSI devono essere terminati attivamente.

Avvertimento

Rimuovere schede SCSI e IDE

Prima di rimuovere una scheda SCSI o IDE, tutte le partizioni dei dispositivi connessi devono essere smontate tramite il comando `umount`. Se si dimentica di farlo, si potrà accedere a questi dispositivi solo dopo un riavvio del sistema.

Avvertimento

14.4 Ulteriori tool

E' stato menzionato più volte il programma cardctl. Questa applicazione è il tool principale per ottenere delle informazioni relative a PCMCIA o per eseguire determinate operazioni. Nella pagina di manuale cardctl (8) trovate ulteriori dettagli; immettendo `cardctl` otterrete un elenco dei comandi validi. Il front- end grafico cardinfo vi permette di controllare le funzioni principali di cardctl. A tal fine deve essere installato `pcmcia-cardinfo`.

Ulteriori tool nel pacchetto `pcmcia` sono `ifport`, `ifuser`, `probe` e `rcpcmcia` che comunque non sono sempre necessari. Per sapere precisamente cosa è contenuto nel pacchetto `pcmcia`, eseguite il comando `rpm -ql pcmcia`.

14.5 Problemi

Finora utilizzare PCMCIA su alcuni notebook o con alcune schede causava dei problemi. La maggior parte delle difficoltà si lasciano risolvere facilmente, se si affronta il problema in modo sistematico. Innanzitutto si deve stabilire se il problema è da ricondurre alla scheda, o se il problema è dovuto al sistema di base PCMCIA. Per tale ragione il computer va in ogni caso avviato in un primo momento senza scheda inserita. Solo se il sistema di base funziona perfettamente, va inserita la scheda. Tutti i messaggi vengono protocollati in `/var/log/messages`. Questo il file va consultato con `tail -f /var/log/messages` durante delle verifiche. Così le possibili cause di errore si lasciano ridurre a due.

14.5.1 Il sistema di base PCMCIA non funziona

Se il sistema si ferma al messaggio PCMCIA: Starting services durante il processo di boot, o se succedono altre cose strane, immettendo `NOPCMCIA=yes` al prompt di boot si evita l'avvio di PCMCIA al prossimo boot. Per circoscrivere maggiormente l'errore, caricate a mano l'uno dopo l'altro i tre moduli di base del vostro sistema PCMCIA.

Per caricare manualmente di moduli PCMCIA, eseguite come `root`: i comandi `modprobe pcmcia_core`, `modprobeyenta_socket` e `modprobe ds`. In rarissimi casi si deve utilizzare al posto di `yenta_socket` uno dei moduli `tcic`, `i82365` o `i82092`. I due moduli ad essere caricati come primi sono i moduli critici.

Se l'errore si verifica durante il caricamento di `pcmcia_core`, potete trovare utili indicazioni nella pagina di manuale di pcmcia_core (4). Le opzioni ivi descritte possono essere testate con il comando `modprobe`. Come esempio verifichiamo i settori I/O liberi. A volte possono verificarsi delle difficoltà se durante il test si vanno a toccare altri componenti hardware. Per evitare delle difficoltà utilizzate l'opzione `probe_io=0`

```
modprobe  pcmcia_core probe_io=0
```

Se l'opzione selezionata conduce al successo, nel file `/etc/sysconfig/pcmcia` la variabile `PCMCIA_CORE_OPTS` va impostata sul valore `probe_io=0`. Se vanno indicate diverse opzioni bisogna separarle da uno spazio:

```
PCMCIA_CORE_OPTS="probe_io=0 setup_delay=10"
```

Se durante il caricamento del modulo `yenta_socket` si verificano degli errori, ciò è spesso dovuto a problemi di natura fondamentale, come l'allocazione delle risorse tramite ACPI.

Inoltre i file `/etc/pcmcia/config` e `/etc/pcmcia/config.opts` vengono elaborati dal gestore delle schede. Le impostazioni ivi fatte sono rilevanti in parte all'avvio di cardmgr ed in parte per il caricamento dei moduli driver per schede PC. In `/etc/pcmcia/config.opts` potete includere o escludere anche IRQ, porte IO e aree della memoria. A volte l'accesso ad un settore I/O errato comporta il crollo del sistema. In questi casi si consiglia di limitare queste aree.

14.5.2 La scheda PCMCIA non funziona bene

Qui esistono in linea di massima tre possibilità: la scheda non viene riconosciuta, il driver non può essere caricato oppure l'interfaccia messa a disposizione dal driver è stata configurata in modo errato. Bisogna inoltre sapere se la scheda viene amministrata dal gestore di schede o dall'hotplug. Il gestore delle schede si occupa di schede PC e l'hotplug di schede CardBUS.

Nessuna reazione all'inserimento della scheda

Se dopo l'inserimento della scheda il sistema non sembra reagire ed anche un `cardctl insert` eseguito manualmente non porta all'esito desiderato, allora può darsi che ci troviamo di fronte ad una allocazione errata degli interrupt ai dispositivi PCI. Spesso anche altri dispositivi PCI come la scheda di rete non funzionano correttamente. In questi casi, provate con il parametro di boot `pci=noacpi` o altri parametri PCI o ACPI

La scheda non viene rilevata Se la scheda non viene rilevata, in `/var/log/messages` vi è il messaggio unsupported Card in Slot x, che vuol dire semplicemente che il gestore delle schede non riesce ad attribuire alcun driver alla scheda. Per poter attribuire un driver sono richiesti i file `/etc/pcmcia/config` o `/etc/pcmcia/*.conf`. Questi file sono per così dire la banca dati di driver che si lascia espandere semplicemente prendendo come modello le registrazioni già presenti. Con il comando `cardctl ident` potete visualizzare ulteriori dettagli inerenti alla scheda. Ulteriori informazioni sono reperibili nel PCMCIA-HOWTO (sezione 6) e nella pagina di manuale pcmcia (5). Dopo aver modificato `/etc/pcmcia/config` o `/etc/pcmcia/*.conf` bisogna ricaricare l'allocazione dei driver con un semplice `rcpcmcia reload`.

Il driver non viene caricato Una possibile causa è che la banca dati dei driver presenta una allocazione errata dovuta ad esempio al fatto che un fornitore abbia integrato in un modello di scheda apparentemente non modificato un altro chip. A volte vi sono dei driver alternativi che in certi modelli funzionano meglio del driver di default. In questi casi servono delle precise informazioni sulla scheda. Anche in questi casi delle mailing list oppure il nostro Advanced Support Service possono essere d'aiuto.

Nel caso di schede cardbus va inserito `HOTPLUG_DEBUG=yes` nel file `/etc/sysconfig/hotplug`. In seguito si avranno nel file di log del sistema dei messaggi che permettono di evincere se il driver è stato caricato (correttamente).

Un'altra possibile causa è rappresentata da un conflitto di risorse. Per la maggioranza delle schede PCMCIA non è rilevante con quale IRQ, porta IO oppure area di memoria vengano utilizzate, ma vi sono anche delle eccezioni. In questi casi testate le schede singolarmente ed eventualmente spegnete temporaneamente anche altre componenti di sistema come scheda audio, IrDA, modem o stampante. L'allocazione delle risorse del sistema può essere visualizzata con `lsdev` (da eseguire come utente `root`). É del tutto normale che diversi dispositivi PCI utilizzano lo stesso IRQ.

Un modo per risolvere il problema potrebbe essere quello di usare una opzione adatta per il modulo del driver della scheda che potrete stabilire con `modinfo`⟨*`driver`* ⟩. Per la maggior parte dei moduli vi è anche una pagina di manuale. `rpm -ql pcmcia | grep man` elenca tutte le pagine di manuale contenute nel pacchetto `pcmcia`. Per testare le opzioni potete scaricare i driver di schede anche manualmente.

Una volta trovata la soluzione, in `/etc/pcmcia/config.opts` può es-

sere consentito o proibito l'utilizzo di determinate risorse. Anche le opzioni per driver di schede trovano qui posto. Se p.es. il modulo `pcnet_cs` deve essere utilizzato esclusivamente con l'IRQ 5, dovete immettere:

```
module pcnet_cs opts irq_list=5
```

Interfaccia non configurata correttamente
In questo caso si consiglia di controllare ancora una volta la configurazione dell'interfaccia con `getcfg` per escludere o eliminare dei eventuali errori di configurazione. A tal fine nel file `/etc/sysconfig/network/config` la variabile `DEBUG` ed in `/etc/sysconfig/hotplug` la variabile `HOTPLUG_DEBUG` vanno impostate su `yes`. Con altre schede, o se questo non risolve il problema, vi è inoltre la possibilità di integrare nello script richiamato dal gestore di schede o dall'hotplug (si veda `/var/log/messages`) la riga `set-vx`. In tal modo ogni comando dello script viene protocollato nel file di log del sistema. Una volta identificato il punto critico nello script, i comandi relativi possono essere immessi e testati anche in un terminale.

14.6 Ulteriori informazioni

Chi è interessato a certi notebook, dovrebbe visitare in ogni caso la Linux laptop home page all'indirizzo: `http://linux-laptop.net`. Un'ulteriore buona fonte di informazione è la home page TuxMobil sotto: `http://tuxmobil.org/`. Troverete oltre a tante utili informazioni anche un laptop-Howto ed un IrDA-Howto. Inoltre vi sono nella banca dati di supporto di SUSE Linux diversi articoli dedicati a questo tema; eseguite ad es. una ricerca con il lemma *Laptop* oppure *notebook* al seguente indirizzo `http://portal.suse.com`.

SCPM: System Configuration Profile Management

Questo capitolo tratta il System Configuration Profile Management (SCPM). L'SCPM consente di adattare la configurazione del vostro sistema a diversi ambienti operativi o configurazioni di hardware. SCPM amministra un set di profili di sistema tagliati per i rispettivi scenari operativi. SCPM permette di passare da un profilo di sistema all'altro senza dover eseguire una riconfigurazione manuale del sistema.

A volte si rende necessario modificare la configurazione di un sistema. Il caso più frequente sarà di certo quello di un portatile utilizzato in ambienti di lavoro diversi; oppure può darsi anche il caso che per un determinato periodo di tempo si utilizza una differente componente di hardware sul desktop. In ogni caso, ritornare allo stato originario del sistema non dovrebbe essere accompagnato da problemi. Preferibilmente, il ripristino della configurazione di origine dovrebbe essere riproducibile senza difficoltà alcuna. Con SCPM è possibile determinare una parte della configurazione del sistema di cui archiviare diversi stati in appositi cosiddetti profili di configurazione.

La configurazione di rete dei portatili sarà probabilmente l'ambito di applicazione principale di SCPM. Comunque c'è da considerare che diverse impostazioni di rete influiscono anche su altri elementi come ad es. sulle impostazioni per la posta elettronica o proxy. C'è da tener in considerazione se in ambito domestico ed in ufficio si utilizzano stampanti diverse, eventualmente bisogna anche avere un occhio di riguardo per la configurazione del beamer (proiettore multimediale), particolari impostazioni per il risparmio energetico da abilitare quando si è in viaggio o in caso di un diverso fuso orario delle filiali all'estero.

15.1 Terminologia

La terminologia riportata di seguito viene utilizzata nella documentazione di SCPM e nel modulo di YaST.

- *Configurazione del sistema* riguarda le principali impostazioni del sistema p.es. l'uso di partizioni del disco rigido, impostazioni di rete, scelta del fuso orario e mappatura della tastiera.
- Un *profilo* detto anche *profilo di configurazione* descrive uno stato della configurazione del sistema, ripreso ad un certo momento, che può essere ripristinato all'occorrenza.
- Il *profilo attivo* indica il profilo attualmente usato. Ciò si riferisce al profilo attualmente selezionato. Ciò non vuol dire che la configurazione del sistema corrisponda esattamente al profilo, poiché la configurazione si lascia modificare in ogni momento.
- *Risorsa*: in relazione all'SCPM le risorse sono tutti quegli elementi che contribuiscono alla configurazione del sistema; può trattarsi di un file o un soft

link, senza escludere i vostri meta-dati, come l'utente, i permessi o il tempo di accesso; si può trattare anche di un servizio di sistema abilitato in un profilo e disabilitato in un altro.

- Le risorse vengono organizzate in cosiddetti *Gruppi di risorse*. Questi gruppi contengono rispettivamente le risorse che formano una unità logica. Per la maggior parte dei gruppi ciò significa la presenza di un servizio e dei rispettivi file di configurazione. Questo meccanismo permette di riunire delle risorse che devono essere gestite da SCPM, senza dover sapere quali file di configurazione sono preposti a quale servizio. SCPM contiene già una preselezione di gruppi di risorse attivati che per la maggioranza dei casi dovrebbe rilevarsi del tutto sufficiente.

15.2 Configurare SCPM dalla linea di comando

Tratteremo di seguito la configurazione dalla linea di comando di SCPM. Mostreremo come avviare, configurare SCPM e come utilizzare i profili.

15.2.1 Lanciare SCPM e definire i gruppi risorsa

Innanzitutto bisogna abilitare SCPM tramite `scpm enable`. Quando abilitate SCPM per la primissima volta il processo di inizializzazione potrà richiedere un paio di secondi. Tramite `scpmdisable` potrete disabilitare SCPM in ogni momento per evitare l'attivazione involontaria di profili. Riabilitando nuovamente SCPM si potrà proseguire senza difficoltà alcuna.

Di solito SCPM viene utilizzato per impostazioni di rete e di stampa nonché per la configurazione di X.Org. Se inoltre desiderate amministrare in questo modo anche dei servizi o file di configurazione, dovete abilitare i rispettivi gruppi di risorsa. Con il comando `scpm list_groups` potete farvi mostrare i . gruppi di risorsa già definiti, se volete farvi mostrare solo i gruppi già abilitati, immettete `scpm list_groups -a`. I comandi devono venir eseguiti come utente `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
```

Potete abilitare o disabilitare i gruppi tramite `scpm activate_group NOME` oppure `scpm deactivate_group NOME`, laddove `NOME` è da sostituire con il relativo nome del gruppo.

15.2.2 Generare e gestire dei profili

Dopo aver abilitato SCPM troverete un profilo di nome `default`. Con `scpm list` ottenete una lista di tutti i profili disponibili. Questo profilo chiaramente è per il momento anche il profilo attivo. `scpm active` vi mostra il profilo attivo. Il profilo `default` è stato concepito come configurazione di base da cui derivare gli altri profili. Per questo motivo eseguite innanzitutto le impostazioni che devono essere applicate in modo uniforme a tutti i profili. Con `scpm reload` le modifiche verranno memorizzate nel profilo attivo. Il profilo `default` può essere rinominato o copiato a piacimento per essere usato come punto di partenza per nuovi profili.

Esistono due possibilità per aggiungere un nuovo profilo. Se il nuovo profilo (diciamo `work`) deve basarsi p.es. sul profilo `default`, immettete `scpm copy default work`. Con `scpmswitch work` entrate nel nuovo profilo per configurarlo. A volte capita che la configurazione del sistema sia stata modificata per determinati motivi e si vuole generare un profilo con questa configurazione. In questi casi immettete `scpm add work` per creare un nuovo profilo e salvare la configurazione del sistema attuale nel profilo `work` e contrassegnarlo come profilo attivo. Con `scpm reload` salvate le modifiche nel profilo `work`.

Ovviamente i profili possono essere rinominati o cancellati tramite i comandi `scpm rename a b` e `scpm delete c`. Per rinominare p.es. `work` in `lavoro` immettete `scpm rename work lavoro` e se intendete cancellarlo di seguito eseguite `scpm delete lavoro`. Il profilo attivo non può essere cancellato.

15.2.3 Passare da un profilo di configurazione all'altro

Come abbiamo visto sopra nel caso di `work` si usa il comando `scpm switch work` per passare da un profilo all'altro. Entrate nel profilo

attualmente attivo per applicare le modifiche apportate alla configurazione del sistema. Ciò corrisponde al comando `scpmreload`.

Una breve descrizione di questo processo favorirà la sua comprensione. Come prima cosa SCPM controlla quali risorse del profilo attivo sono state modificate dall'ultimo passaggio da un profilo all'altro. Dalla lista delle risorse modificate viene generata una lista dei gruppi risorsa modificati. Per ogni gruppo modificato verrà chiesto se la modifica dovrà essere assunta o meno anche dal profilo ancora attivo. Se preferite un elenco a parte delle risorse (come nel caso delle versioni precedenti di SCPM) eseguite il comando switch con il parametro `-r`, ovvero: `scpmswitch -r work`.

```
scpm switch -r work

Checking for modified resources
Checking for Resources to be started/shut down
Checking for dependencies
Restoring profile default
```

In seguito SCPM confronta la configurazione del sistema attuale con il nuovo profilo da attivare. Viene stabilito quali servizi di sistema devono essere fermati o (ri)avviati a causa delle modifiche alla configurazione o a causa di dipendenze reciproche. In parte, questo processo ricorda il riavvio di un sistema, solo che in questo caso tale processo coinvolge solamente una piccola parte del sistema mentre il resto del sistema continua a funzionare in modo immutato. Solo a questo punto vengono fermati i servizi di sistema, salvate tutte le risorse modificate (p.es. file di configurazione) e riavviati i servizi di sistema.

15.2.4 Impostazioni per esperti

Per ogni profilo potete aggiungere una descrizione che verrà anche visualizzata con `scpm list`. Per aggiungere una descrizione del profilo che è attualmente attivo, usate il comando `scpm set description "testo"`. Per profili inattivi dovete indicare inoltre il profilo, dunque `scpmset description "testo" work`. Può verificarsi il caso che durante il passaggio da un profilo all'altro debbano essere eseguite delle azioni aggiuntive non (ancora) contemplate da SCPM. Per realizzare questo potete integrare per ogni profilo quattro programmi o script eseguibili che verranno inizializzati nelle diverse fasi di un passaggio da un filtro all'altro. Queste fasi sono:

prestop prima di fermare dei servizi al momento del passaggio tra i profili

poststop dopo l'arresto dei servizi al momento del passaggio tra i profili

prestart prima dell'avvio dei servizi al momento di attivare il profilo

poststart dopo l'avvio dei servizi al momento di attivare il profilo

Queste azioni possono essere eseguite con il comando `set`, cioè con `scpm set prestop nomefile`, `scpmset poststop nomefile`, `scpm set prestart nomefile` o `scpm set poststart nomefile`. Si deve trattare di un programma eseguibile, cioè gli script devono far riferimento all' interpreter corretto.

Avvertimento

Integrare propri script

Gli script che dovranno essere eseguiti da SCPM devono essere leggibili ed eseguibili per il superutente (`root`). Questi script non dovrebbero essere accessibili per utenti normali. Tramite `chmod700 nomefile` e `chown root:root nomefile` date a `root` la sovranità esclusiva sul file in questione.

Avvertimento

Tutte le impostazioni aggiuntive che sono state immesse con `set`, possono essere visualizzate con `get`. Per esempio `scpmget poststart` fornisce il nome del comando poststart o nessuna informazione se non è stato aggiunto alcunché. Le impostazioni si cancellano sovrascrivendole con `""`; ad esempio `scpm set prestop ""` rimuove nuovamente il programma prestop.

Come per le descrizioni, tutti i comandi `set` e `get` possono essere applicati ad un profilo qualsiasi. Basta aggiungere il nome del profilo. Per esempio `scpmget prestop nomefile work` o `scpmget prestop work`.

15.3 YaST: il gestore dei profili

Avviate il modulo Gestione profili di YaST ('Sistema' → 'Gestione profili'). Al primo avvio abilitate esplicitamente SCPM selezionando 'Abilita' nella finestra 'Opzioni SCPM', mostrata nella figura 15.1 nella pagina successiva. Sotto 'Impostazioni' determinate se volete o meno visualizzare i messaggi dettagliati

riguardo allo stato di avanzamento del processo configurativo di SCPM. Sotto 'Modalità di passaggio', specificate se le risorse modificate del profilo attivo debbano essere salvate o scartate quando si esegue il passaggio di profilo. Se qui selezionate 'Normale', tutte le modifiche nel profilo attivo verranno salvate al passaggio. Potete definire il comportamento di SCPM al momento del boot, impostando il 'Modo di boot' su 'Salva modifiche' (impostazione di default) o su 'Abbandona modifiche'.

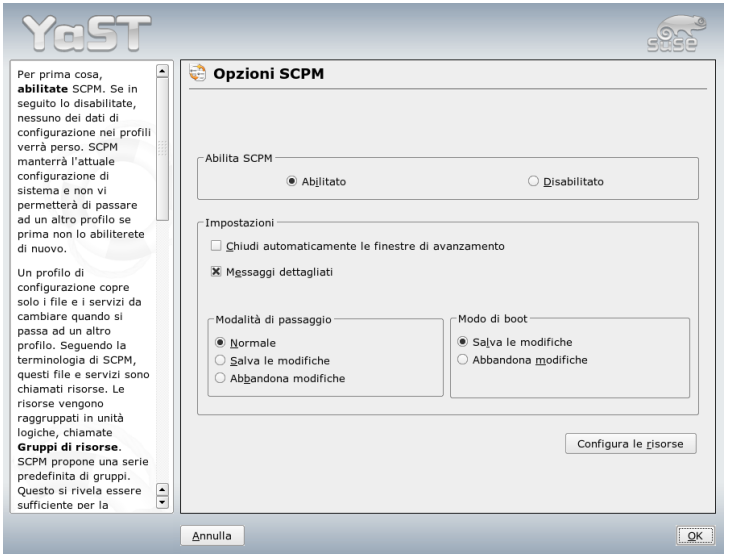

Figura 15.1: *YaST Opzioni SCPM*

15.3.1 Configurare gruppi di risorsa

Per apportare delle modifiche all'attuale configurazione delle risorse selezionate 'Configura risorse' nella finestra 'Opzioni SCPM'. Nella prossima finestra, 'Configurazione dei gruppi risorsa' (riportata nella figura 15.2 nella pagina seguente), verranno elencati tutti i gruppi risorsa disponibili del vostro sistema. Per aggiungere o modificare un gruppo risorsa, specificate o modificate 'Gruppo risorsa' e 'Descrizione' (nel caso di un servizio LDAP, ad esempio, indicate `ldap` quale 'Gruppo risorsa' e `Servizio client LDAP` come 'Descrizione'). Specificate

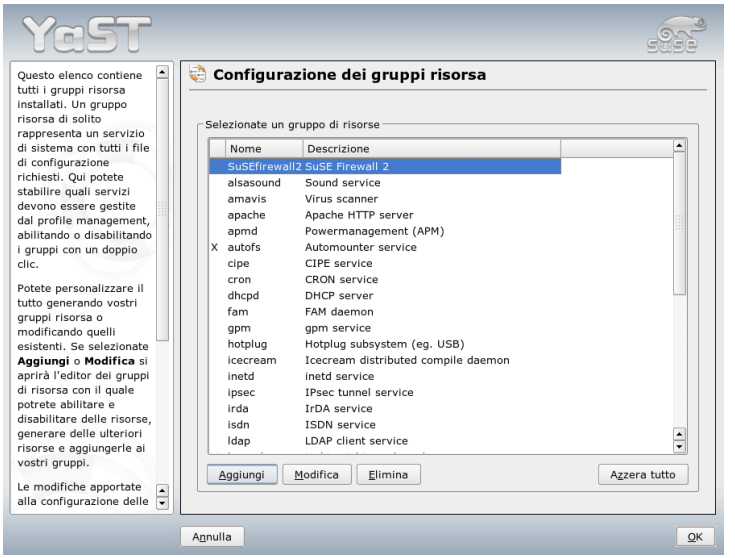

Figura 15.2: *Configurazione gruppi risorse*

quindi le risorse del caso (servizi, file di configurazione, o entrambi) o modificate quelle esistenti. Eliminate quelle che non vengono utilizzate. Per ripristinare lo stato delle risorse selezionate — e azzerare ogni modifica apportata per ristaurare i valori iniziali— selezionate 'Ripristina gruppo'. Le modifiche vengono salvate nel profilo attivo.

15.3.2 Creare un nuovo profilo

Se volete creare un nuovo profilo, cliccate su 'Aggiungi' nella finestra iniziale ('Gestione dei profili di configurazione di sistema'). Nella finestra che si apre, stabilite se il nuovo profilo debba basarsi sulla configurazione di sistema attuale (SCPM rileva automaticamente la configurazione attuale e la salva nel vostro profilo) o su un profilo esistente. Se decidete di utilizzare la configurazione di sistema attuale come base del nuovo profilo, potete contrassegnare il nuovo profilo come il nuovo profilo attivo. Ciò non va ad influire sul vecchio profilo e non avvia né ferma alcun servizio.

Indicate un nome e una breve descrizione per il nuovo profilo nella finestra successiva. Se SCPM debba eseguire degli script speciali al passaggio da un profilo all'altro, specificate il percorso di ogni eseguibile (si veda la figura 15.3 in questa pagina). Consulate la sezione 15.2.4 a pagina 299 per maggiori informazioni. SCPM esegue una verifica delle risorse del nuovo profilo. Se la verifica viene portata a termine correttamente potrete utilizzare immediatamente il nuovo profilo.

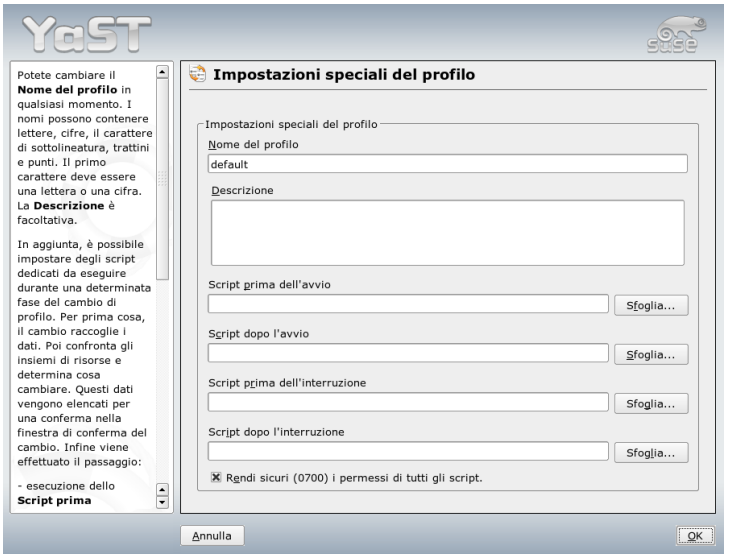

Figura 15.3: *Impostazione del profilo speciali*

15.3.3 Modificare profili esistenti

Potete modificare un profilo esistente selezionando 'Modifica' nella finestra iniziale ('Gestione dei profili di configurazione di sistema'). Quindi potete modificare nome, descrizione, script e risorse in base alle vostre esigenze.

15.3.4 Passare da un profilo all'altro

Per eseguire un passaggio tra profili, lanciate il gestore dei profili. Il profilo attivo è contrassegnato con una freccia. Selezionate il profilo a cui passare e cliccate su 'Passa a'. SCPM verifica la presenza di risorse nuove o modificate e all'occorrenza le aggiunge.

Se una risorsa ha subito una modifica, YaST apre la finestra 'Conferma passaggio'. 'Gruppi risorse modificati del profilo attivo' elenca tutti i gruppi risorsa di un profilo attivo modificati ma non ancora salvati nel profilo attivo. Tramite 'Salva o ignora' determinate per il gruppo risorsa attualmente selezionato se le modifiche apportate a questo gruppo risorsa vanno salvate o meno nel profilo attivo. Alternativamente potete selezionare ogni singola risorsa e cliccare su 'Dettagli' per avere maggiori informazioni. Verrà mostrato un elenco dei file di configurazione o degli eseguibili appartenenti al gruppo risorsa in questione che sono stati modificati. Se volete confrontare ogni rigo della nuova e vecchia versione cliccate su 'Mostra modifiche'. Dopo averle visualizzate tramite 'Azione' potete stabilire cosa fare:

Salva risorsa salvare la risorsa nel profilo attivo lasciando immutati tutti gli gli altri profili

Ignora risorsa non apportare delle modifiche alla risorsa attiva. Questa modifica non verrà applicata.

Salva in ogni profilo copiare l'intera configurazione della risorsa negli altri profili.

Correzione di tutti i profili applicare solo le più recenti modifiche a tutti i profili.

Tramite 'Salva o ignora tutto' decidete cosa fare delle modifiche apportate alle risorse mostrate in questa finestra.

Dopo aver confermato le modifiche relative al profilo attivo, uscite dalla finestra 'Conferma passaggio' cliccando su 'OK'. SCPM quindi effettuerà il passaggio al nuovo profilo. Durante il passaggio, SCPM esegue gli script prestop e poststop del vecchio profilo e gli script prestart e poststart per il nuovo profilo.

15.4 Difficoltà e la loro risoluzione

Segue una breve rassegna delle difficoltà riscontrate frequentemente con SCPM. Ecco come sorgono e come risolverle.

15.4.1 Interruzione del passaggio di profilo

Eventualmente può verificarsi il caso che SCPM si interrompa durante il passaggio da un profilo all'altro. Ciò può essere dovuto a motivi esterni - p.es. interruzione tramite l'utente, batteria scarica del portatile - oppure ad un errore in SCPM. In ogni caso, la prossima volta che invocate SCPM, il sistema vi comunicherà che SCPM è bloccato. Questa funzionalità è stata ideata per proteggere il vostro sistema, visto che possono esserci delle discrepanze tra i dati memorizzati nella banca dati di SCPM e lo stato del vostro sistema. In questi casi eseguite un `scpm recover`. SCPM esegue tutte le operazioni non eseguite in precedenza. Potete anche ricorrere a `scpm recover -b`, per annullare le operazioni eseguite in precedenza. Se utilizzate il gestore dei profili YaST, all'avvio appare un dialogo in cui poter eseguire i comandi sopramenzionati.

15.4.2 Modificare la configurazione del gruppo risorsa

Tramite `scpm rebuild` potete modificare - a SCPM già inizializzato - la configurazione del gruppo risorsa, dopo aver terminato di aggiungere o eliminare dei gruppi. Verranno aggiunte nuove risorse a tutti i profili e cancellate definitivamente quelle eliminate. Se le risorse modificate sono state configurate in modo diverso nei diversi profili, andranno persi i rispettivi file di configurazione - fatta eccezione chiaramente per la versione attuale del vostro sistema, che non viene toccata da SCPM. Se modificate la configurazione con YaST, non è necessario eseguire un rebuild, YaST lo farà automaticamente.

15.5 Selezionare un profilo al boot del sistema

Per selezionare un profilo al boot del sistema, premete (F4) durante il processo di boot (schermata di boot) per poter accedere ad un elenco dei profili disponibili. Tramite i tasti freccia potete fare la vostra selezione e con (Invio) confermare la vostra selezione. Il profilo selezionato verrà utilizzato d'ora in poi come opzione di boot.

15.6 Ulteriori informazioni

La documentazione aggiornata si trova nelle pagine info di SCPM che possono essere consultate con Konqueror o Emacs (`konqueror info:scpm`). Sulla console si usa `info` o `pinfo`. La documentazione per gli sviluppatori è reperibile sotto `/usr/share/doc/packages/scpm`.

Il power management

Questo capitolo presenta una rassegna dei diversi modi di realizzare il risparmio energetico (power management) sotto Linux. Segue una descrizione dettagliata della configurazione di tutte le tecniche possibili: dall' APM (ingl. Advanced Power Management) e ACPI (ingl. Advanced Configuration and Power Interface) fino ad arrivare al CPU Frequency Scaling.

Dal puro power management su portatili con APM si è passato allo sviluppo di ACPI che rappresenta un tool per la configurazione delle informazioni di hardware per computer moderni (portatili, desktop e server). Numerose componenti di hardware moderni consentono di adattare la frequenza di CPU alle condizioni specifiche di un dato momento, cosa che aiuta a realizzare un rilevante risparmio energetico in particolar modo su dispositivi mobili quando vengono alimentati dalla batteria (*CPU Frequency Scaling*).

Il power management presuppone hardware adatto e routine BIOS adatte. La maggior parte dei portatili e tanti desktop e server moderni presentano i presupposti per consentire il power management. Su hardware non proprio recentissimo spesso si è usato lo standard APM (Advanced Power Management). Visto che l'APM consiste in fondo di una serie di funzioni implementate nel BIOS, il supporto ad APM non funziona su tutti i dispositivi nello stesso modo. ACPI è più complesso e il supporto da parte dell'hardware varia ancora di più che per l'APM. Per tale ragione non ha senso propagare l'uno o l'altro sistema. Eseguite dei test col vostro hardware e adottate la tecnologia che meglio si addice al vostro ambiente.

Importante

Power management su processori AMD64

I processori AMD64 supportano in combinazione con un kernel a 64 bit esclusivamente l' ACPI.

Importante

16.1 Funzionalità di risparmio energetico

Queste funzioni sono di interesse non solo per portatili ma anche per sistemi desktop. Descriveremo queste funzioni e ne spiegheremo l'utilizzo per i due sistemi di power management, ovvero APM e ACPI.

Stand-by In questo stato operativo è solo il display ad essere spento e viene ridotta l'attività del processore. Non tutte le implementazioni di APM mettono a disposizione questa funzionalità che corrisponde allo stato S1 o S2 dell'ACPI.

Suspend (to memory) Lo stato del sistema viene scritto per intero sulla RAM e viene sospeso il funzionamento del resto del sistema. Il computer consuma

così poca energia ed, in base al computer, la batteria può durare da 12 ore fino ad arrivare a diversi giorni. Il vantaggio è che entro pochi secondi si può continuare a lavorare da dove si era smesso senza dover riavviare il sistema o ricaricare gli applicativi richiesti. Con la maggior parte dei dispositivi moderni basta abbassare il display per entrare nella modalità sospensione in memoria (suspend to memory) e rialzarlo per continuare a lavorare. Corrisponde grosso modo allo stato S3 dell'ACPI. Per quanto riguarda il supporto di questa modalità, tutto dipende dall' hardware utilizzato.

Hibernation (suspend to disk) Qui lo stato del sistema viene salvato sul disco fisso ed in seguito spento il sistema. Ci vogliono tra 30 e 90 secondi prima che il computer si risvegli dallo stato di ibernazione e per tornare precisamente allo stato antecedente all'ibernazione. Alcune case produttrici offrono nel loro APM un variante interessante (p.es. RediSafe dei Thinkpads di IBM). Questa funzione corrisponde allo stato S4 dell'ACPI. In Linux la *Sospensione su disco* viene gestita dalle routine del kernel che non dipendono dall'APM o ACPI.

Controllo dello stato della batteria ACPI e APM vegliano e informano sullo stato di caricamento della batteria. Inoltre coordinano l'esecuzione di determinate operazioni quando la batteria segnala un livello di caricamento critico.

Spegnimento automatico Dopo lo shutdown il computer viene completamente spento. Funzionalità importante soprattutto quando viene eseguito uno shutdown automatico poco prima che la batteria sia completamente scarica.

Spegnimento di componenti del sistema
Quando si tratta di risparmio energetico è il disco rigido a svolgere e un ruolo fondamentale. A seconda della affidabilità del sistema, il disco rigido può venir sospeso per un determinato periodo di tempo. Comunque aumenta il rischio che vadano persi dei dati proporzionalmente alla durata della sospensione del disco rigido. Altre componenti possono essere disattivate tramite ACPI almeno in teoria temporaneamente o permanentemente nel BIOS setup.

Controllo dell'attività del processore In riferimento alla CPU si può realizzare un risparmio energetico in tre modi: intervenendo sulla frequenza ed il voltaggio della CPU (procedimenti noti anche sotto il nome di PowerNow! o Speedstep), throttling - ovvero riduzione della frequenza di clock - e mandando in sospensione il processore (cosiddetti stati C). In base al modo operativo del sistema questi tre approcci possono essere combinati.

16.2 APM

Alcune funzionalità di risparmio energetico vengono eseguite in modo autonomo dal BIOS APM. Spesso gli stati di stand-by e suspend si lasciano attivare con una combinazione di tasti o abbassando il display. In questi casi non è necessaria alcuna funzionalità del sistema operativo. Per poter attivare questi modi tramite un comando devono venire eseguite delle particolari azioni prima che si ha la sospensione dell'attività del sistema. Per visualizzare il livello caricamento della batteria, devono essere installati i relativi pacchetti ed il kernel adatto.

Nei kernel di SUSE LINUX il supporto APM è integrato e viene attivato solamente se nel BIOS non è implementato alcun ACPI ed è stato rilevato un APM BIOS. Per attivare il supporto a APM, bisogna spegnere ACPI al prompt di boot con `acpi=off`. Potete controllare con il comando `cat /proc/apm` se l'APM è abilitato. Se viene indicata una riga con diversi numeri, allora tutto è a posto. Immettendo a questo punto `shutdown -h` il computer dovrebbe spegnersi.

Visto che alcune implementazioni BIOS non si attengono esattamente agli standard, a volte si verificano dei comportamenti strani. Alcuni problemi si lasciano risolvere con dei particolari parametri di boot (prima vi erano delle opzioni di configurazione del kernel). Tutti i parametri vengono immessi al prompt di boot sotto forma di `apm=parametro`:

on/off Abilitare/disabilitare il supporto APM

(no-)allow-ints Permettere degli interrupt durante l'esecuzione delle funzioni BIOS.

(no-)broken-psr La funzione "GetPowerStatus" del BIOS non funziona correttamente.

(no-)realmode-power-off Riportare il processore prima dello shutdown nella modalità reale (real mode).

(no-)debug Protocollare gli eventi APM nel syslog.

(no-)power-off Spegnere il sistema dopo lo shutdown.

bounce-interval=⟨*n*⟩ Tempo espresso in centesimi di secondo, in cui vengono ignorati ulteriori eventi di sospensione dopo il verificarsi di un evento di sospensione.

idle-threshold=⟨*n*⟩ Percentuale della attività del sistema, a partire della quale viene richiamata la funzione BIOS `idle` (0=sempre, 100=mai).

idle-period=⟨*n*⟩ Centesimi di secondo in cui viene misurata l'(in)attività del sistema.

apmd (l'APM daemon) è caduto in disuso visto che le sue funzionalità sono contenute nel nuovo powersaved che inoltre armonizza bene con ACPI e permette di regolare la frequenza della CPU.

16.3 ACPI

ACPI sta per *Advanced Configuration and Power Interface*. ACPI permette al sistema operativo di configurare e controllare le singole componenti hardware. In tal maniera ACPI sostituisce sia il "plug and play" che l' APM. In più l'ACPI fornisce una serie di informazioni riguardanti la batteria, la temperatura, l'alimentatore e la ventola nonché segnala eventi di sistema del tipo "Abbassare il display" o "Batteria quasi scarica".

Il BIOS mette a disposizione delle tabelle in cui reperire i dati sulle singole componenti e sui metodi per accedere all'hardware. Il sistema operativo utilizza queste informazioni per assegnare ad es. degli interrupt oppure per accendere e spegnere delle componenti. Visto che il sistema operativo esegue istruzioni che si trovano nel BIOS anche qui molto dipende dalla implementazione del BIOS. In `/var/log/boot.msg` trovate i messaggi di boot, le tabelle rilevate e lette correttamente da ACPI. Per maggiori informazioni sul modo di risolvere dei problemi dovuti all'ACPI rimandiamo alla sezione 16.3.4 a pagina 316.

16.3.1 Nella prassi

Se all'avvio il kernel rivela un ACPI BIOS, l' ACPI verrà abilitato automaticamente (ed l'APM disabilitato). Il parametro di avvio `acpi=on` è richiesto al massimo con macchine datate. Chiaramente il computer dovrà supportare ACPI 2.0 o versioni successive. Nei messaggi di boot del kernel in `/var/log/boot.msg`

In seguito bisogna caricare una serie di moduli. Questi vengono caricati dallo script di avvio del demone di ACPI. Se uno di questi moduli dovesse creare dei problemi, in `/etc/sysconfig/powersave/common` potrete stabilire se caricarlo o meno. Nel file di log del sistema (`/var/log/messages`) vedete le comunicazioni dei moduli e si può vedere quali componenti sono state rilevate.

A questo punto sotto `/proc/acpi` avrete una serie di file che vi informano sullo stato del sistema o grazie ai quali è possibile intervenire attivamente su determinati stati. Comunque alcune funzionalità non funzionano in modo ineccepibile visto che si trovano ancora nello stato sperimentale e dipendono dalla implementazione del produttore.

Tutti i file (tranne `dsdt` e `fadt`) possono essere letti con `cat`. Si possono modificare le impostazioni di alcuni di questi file passando con `echoX file` dei valori appropriati per X. Per poter accedere a queste informazioni e intervenirvi, utilizzate sempre il comando `powersave`. Per una migliore comprensione ecco i file più importanti:

`/proc/acpi/info` Informazioni generali su ACPI

`/proc/acpi/alarm` Qui potete impostare quando si debba risvegliare il sistema. Attualmente comunque questa funzionalità non è ancora sufficientemente supportata.

`/proc/acpi/sleep` Informa sui possibili stati di sleep.

`/proc/acpi/event` Qui vengono segnalati tutti gli eventi che vengono elaborati dal demone `powersaved`. Se non vi accede alcun demone, gli eventi possono essere visualizzati con `cat /proc/acpi/event` (terminare con Ctrl-C), eventi appartenenti a questa categoria si hanno ad esempio quando si preme brevemente sul pulsante per l'accensione del sistema o quando si abbassa il display.

`/proc/acpi/dsdt` e **`/proc/acpi/fadt`**
Qui trovate le tabelle ACPI: DSDT (*Differentiated System Description Table*) e FADT (*Fixed ACPI Description Table*) che possono essere lette con `acpidmp`,`acpidisasm` e `dmdecode`. Questi programmi e la relativa documentazione si trovano nel pacchetto `pmtools`. Esempio: `acpidmpDSDT | acpidisasm` .

`/proc/acpi/ac_adapter/AC/state`
L'alimentatore è connesso?

`/proc/acpi/battery/BAT*/{alarm,info,state}`
Informazioni dettagliate sullo stato della batteria. Per vedere quanto sia carica la batteria bisogna confrontare `last full capacity` di `info` con `remaining capacity` di `state` oppure ricorrere a dei programmi speciali che vengono illustrati nella sezione 16.3.3 a pagina 316. In `alarm` potete impostare il valore che innesca un evento di batteria.

/proc/acpi/button Qui trovate delle informazioni sui vari bottoni.

/proc/acpi/fan/FAN/state Indica se la ventola è in funzione. Essa può venir accesa o spenta manualmente immettendo in questo file `0` (=on) o `3` (=off). Comunque dovete considerare che sia il codice ACPI nel kernel che l'hardware (o il BIOS) possono sovrascrivere questa impostazione se vi è surriscaldamento.

/proc/acpi/processor/CPU*/info
Informazioni sulle possibilità di risparmio energetico per il processore.

/proc/acpi/processor/CPU*/power
Informazioni sullo stato attuale del processore. Un asterisco vicino a `C2` sta per inattività; questo è lo stato più frequente, come mostra la cifra `usage`.

/proc/acpi/processor/CPU*/throttling
Qui potete impostare il throttling del processore. Spesso sono previsti otto livelli di throttling, indipendentemente dagli interventi sulla frequenza della CPU.

/proc/acpi/processor/CPU*/limit
Se un demone regola automaticamente la performance ed il throttling, qui potete impostare i limiti che non devono essere superati. Vi sono dei limiti stabiliti dal sistema e limiti impostabili dall'utente.

/proc/acpi/thermal_zone/ Qui vi è una sottodirectory per ogni zona termica; una zona termica è un settore con simili caratteristiche termiche, il cui numero e la cui denominazione li stabilisce il produttore. Le tante possibilità offerte da ACPI spesso non vengono implementate. Di solito il controllo termico viene effettuato direttamente dal BIOS senza che il sistema abbia voce in capitolo, visto che si tratta niente popo di meno della possibile durata del vostro hardware. Le descrizioni che seguono sono in parte meramente di natura teorica.

/proc/acpi/thermal_zone/*/temperature
La temperatura attuale della zona termica.

/proc/acpi/thermal_zone/*/state
Indica se tutto è `ok` o se l'ACPI raffredda in modo `attivo` o `passivo`. Lo stato è `ok` se il controllo della ventola non dipende dall'ACPI.

/proc/acpi/thermal_zone/*/cooling_mode
: Qui si può selezionare il metodo di raffreddamento preferito gestito dall'ACPI: passivo (meno performance, ma risparmio considerevole) o attivo (sempre a tutta potenza e ventola al massimo).

/proc/acpi/thermal_zone/*/trip_points
: Qui potete impostare a partire da quale temperatura si debba intervenire. Si va dal raffreddamento attivo o passivo, alla sospensione (`hot`) fino allo spegnimento del computer (`critical`). Le possibili azioni da eseguire variano da dispositivo a dispositivo e sono definite nel DSDT. I trip point, ossia valori soglia, stabiliti nella specificazione ACPI sono: `critical`, `hot`, `passive`, `active1` ed `active2`. Anche se non sono implementati tutti, vanno indicati in questa sequenza nel file `trip_points`. Ad esempio `echo 90:0:70:0:0 >trip_points` imposta il limite di temperatura per `critical` su `90` e per `passive` su`70`.

/proc/acpi/thermal_zone/*/polling_frequency
: Se il valore `temperature` non viene aggiornato automaticamente, non appena cambia la temperatura si può passare al "modo polling". Il comando `echo X > /proc/acpi/thermal_zone/*/polling_frequency` fa sì che l'indicazione della temperatura venga aggiornata ogni `X` secondi. Con `X=0` si disabilita nuovamente il "polling".

Per le impostazioni, dati ed eventi summenzionati non è necessario apportare delle modifiche manualmente. Vi è a riguardo il daemon powersave (powersaved) ed una serie di applicazioni tra cui powersave, kpowersave e wmpowersave. Si veda la sezione 16.3.3 a pagina 316. Dato che powersaved include le funzionalità di acpid, acpid diventa obsoleto.

16.3.2 Controllo del livello di attività del processore

La CPU conosce tre modi per realizzare il risparmio energetico, che possono essere combinati in base al modo operativo del sistema. Il risparmio energetico comporta anche un minor livello di riscaldamento del sistema e quindi ridotta attività della ventola.

Frequenza e voltaggio PowerNow! e Speedstep sono delle espressioni coniate da AMD e Intel per definire questo tipo di funzionalità, che comunque è presente anche su processori di altri produttori. Tramite queste funzionalità viene ridotta la frequenza di clock e il voltaggio della CPU. Il vantaggio derivante è che si realizza un risparmio energetico che va oltre ad una

progressione lineare. Tradotto in altri termini: con una frequenza ridotta della meta che corrisponde ad un livello di performance dimezzato si realizza un risparmio energetico decisamente oltre al 50%. Questa funzionalità è indipendente dall' APM o ACPI e richiede la presenza di un daemon, che interviene sulla frequenza ed i livelli di performance richiesti in un dato momento. Per eseguire delle impostazioni andate nella directory `/sys/devices/system/cpu/cpu*/cpufreq/`.

Throttling In questo caso viene ignorata una determinata percentuale di impulsi. Con un throttling del 25% viene ignorato ogni quarto impulso, con un throttling del 87,5% solo ogni ottavo impulso raggiunge il processore. Il livello di risparmio energetico realizzato non è lineare. Il throttling trova applicazione in quei casi in cui non vi è altro modo di regolare la frequenza della cpu o per realizzare il massimo in termini di risparmio energetico. Per gestire questo processo vi è `/proc/acpi/processor/*/throttling`.

Stato di sleep del processore Il processore viene indotto dal sistema operativo in uno stato per così dire di dormiveglia ogni volta che vi è inattività. In questi casi il sistema operativo invia alla CPU l'istruzione `halt`. Vi sono diversi livelli di sleep: C1, C2 e C3. Lo stato con il maggior risparmio è C3, nel quale la cache del processore non viene addirittura neanche sincronizzata con la RAM, ragione per cui il sistema può entrare in questo stato solo se non vi è nessun dispositivo che con la sua attività al master bus modifica il contenuto della RAM. Alcuni driver impediscono perciò l'utilizzo di C3. Lo stato attuale viene indicato in `/proc/acpi/processor/*/power`.

Sia la riduzione della frequenza che il throttling hanno senso se applicati con il processore sotto carico, durante fasi di inattività si entra in ogni caso negli stati C volti al risparmio. A CPU attiva la riduzione della frequenza rappresenta la soluzione da preferire ai fini del risparmio energetico. Spesso il processore non lavora toccando i propri limiti, in questi casi basta ridurre la frequenza. Per un adattamento dinamico della frequenza si consiglia di ricorrere ad un daemon (ad es. powersaved). Se il sistema viene alimentato a batteria o se il computer debba raffreddarsi o operare silenziosamente si consiglia di impostare stabilmente una frequenza bassa.

Si dovrebbe ricorrere al throttling solo come ultima possibilità, ad esempio se si vuole prolungare il più possibile la durata della batteria con il sistema sotto pieno carico. Alcuni sistemi però presentano delle disfunzione se vi è un throttling troppo elevato. Con una CPU quasi a riposo non si trae alcun beneficio dal throttling.

Sotto SUSE LINUX queste funzionalità vengono gestite dal deamon powersave. La configurazione richiesta viene illustrata in una sezione propria (si veda la sezione 16.5 a pagina 319).

16.3.3 Ulteriori tool

Vi è una serie di strumenti ACPI più o meno estesi, tra cui una serie di tool di informazione che mostrano lo stato della batteria, temperatura etc.: (acpi, klaptopdaemon, wmacpimon, etc.). Alcuni semplificano l'accesso alle strutture sotto `/proc/acpi` oppure consentono di osservare le variazioni (akpi, acpiw, gtkacpiw). Inoltre vi sono dei tool per editare le tabelle ACPI nel BIOS (il pacchetto `pmtools`).

16.3.4 Possibili problemi e la loro risoluzione

Potrebbero esserci degli errori passati inosservati nel codice ACPI del kernel, comunque in questi casi - non appena vengono scoperti - sarà messa disposizione la correzione da poter scaricare da Internet. Problemi più spinosi e che si verificano più spesso sono dei problemi da ricondurre al BIOS. A volte succede il BIOS presenta delle discrepanze rispetto alla specificazione ACPI per aggirare degli errori nella implementazione ACPI di altri sistemi operativi largamente diffusi. Vi è anche dell'hardware riportato in cosiddette black list che a causa di gravi errori nella implementazione ACPI non può essere utilizzato con l'ACPI del kernel Linux.

Dunque se dovessero verificarsi delle difficoltà si dovrebbe innanzitutto aggiornare il BIOS. Tante difficoltà si risolvono in questa maniera da sé. Se si verificano delle difficoltà durante il boot, provate con uno dei seguenti parametri di avvio:

pci=noacpi non usare ACPI per la configurazione di dispositivi PCI.

acpi=oldboot usare ACPI solo per eseguire una semplice configurazione delle risorse.

acpi=off disabilitare ACPI.

Avvertimento

Difficoltà all'avvio senza ACPI

Alcuni computer recenti, soprattutto sistemi SMP ed AMD64, richiedono l'ACPI ai fini di una corretta configurazione dell'hardware. Disabilitare l'ACPI in questi casi può comportare delle difficoltà.

Avvertimento

Analizzate in questi casi i messaggi di boot, utilizzate a riguardo per esempio il comando `dmesg | grep -2i acpi` (o tutti i messaggi, poiché il problema non è necessariamente legato all'ACPI). Se si verifica un errore durante la lettura di una tabella ACPI potrete sostituire la tabella più importante, la DSDT, con una versione ottimizzata. In tal modo viene ignorata la tabella DSDT del BIOS che contiene degli errori. La procedura da seguire viene illustrata nella sezione 16.5.4 a pagina 325.

Nella configurazione del kernel potrete abilitare le comunicazioni di debug dell'ACPI, una volta compilato ed installato un kernel con ACPI debugging, le informazioni dettagliate raccolte saranno di aiuto a coloro (esperti) che cercheranno di individuare l'errore.

Comunque nel caso di problemi dovuti al BIOS o all'hardware è sempre bene rivolgersi al produttore, anche se non potrà aiutarvi per Linux, comunque noterà che sono sempre più gli utenti che usano Linux e prenderà la questione sul serio.

Ulteriore documentazione

Ulteriore documentazione e assistenza in tema di ACPI:

- `http://www.cpqlinux.com/acpi-howto.html` (ACPI HowTo più dettagliato con delle patch per DSDT)
- `http://www.intel.com/technology/iapc/acpi/faq.htm` (ACPI FAQ @Intel)
- `http://acpi.sourceforge.net/` (Il progetto ACPI4Linux di Sourceforge)
- `http://www.poupinou.org/acpi/` (DSDT Patch di Bruno Ducrot)

16.4 Un breve intervallo per il disco rigido

Linux vi permette di spegnere il disco rigido quando non vi serve o di utilizzarlo in una modalità in cui si realizza il maggior risparmio energetico possibile o il minor rumore possibile. Da quanto abbiamo potuto appurare con moderni notebook non si trae alcun beneficio se si spegne anche solo temporaneamente il disco, dato che entra già da sé in un modo operativo volto alla parsimonia quando viene utilizzato appena. Per chi vuole realizzare comunque il massimo in termini di risparmio può provare quanto illustrato di seguito. La maggior parte delle funzionalità si lascia gestire tramite powersaved.

Per eseguire diverse impostazioni riguardanti il disco rigido vi è il programma hdparm. Con l'opzione `-y` il disco rigido viene mandato immediatamente in stand-by con `-Y` (Attenzione!) viene spento completamente. Con `hdparm -S x;` spegnete il disco rigido dopo un certo periodo di inattività. Il segnaposto $\langle x \rangle$ assume a secondo del valore immesso i seguenti significati: `0` disabilita questo meccanismo, il disco è sempre in esecuzione. I valori da `1` a `240` devono essere moltiplicati con 5 secondi. `241 - 251` corrispondono a 1 fino a 11 volte 30 minuti.

Possibilità di risparmio proprie dei dischi vengono gestite tramite l'opzione `-B`. Con una cifra tra `0` e `255` si va dal massimo in termini di risparmio al massimo in termini della velocità di trasmissione dei dati. I risultati ottenuti dipendono dal disco utilizzato. Per rendere un disco meno rumoroso si può utilizzare l'opzione `-M`. Tramite i valori compresi fra `128` e `254` si seleziona tra rumorisità e velocità.

Spesso però non è facile mettere a riposo il disco rigido, visto che sotto Linux vi sono numerosi processi che scrivono dei dati sul disco e quindi lo "svegliano" continuamente. Così a questo punto cercheremo di capire il modo in cui vengono gestiti i dati da scrivere sul disco sotto Linux. Tutti i dati vengono salvati temporaneamente nel buffer della RAM. Il buffer viene controllato dal "Kernel Update Daemon" (kupdated). Ogni volta che i dati raggiungono un determinato periodo di permanenza o la parte occupata del buffer raggiunge un certo livello, il buffer si svuota e i dati vengono trasferiti sul disco rigido. La dimensione del buffer è tra l'altro dinamica e dipende dalla quantità di memoria e dal carico del sistema. Visto che la sicurezza dei dati è l'obiettivo principale, kupdated è impostato di default su intervalli brevi. Ogni 5 secondi esegue un controllo del buffer e informa il demone bdflush se vi sono dei file con una permanenza di oltre 30 secondi o se il buffer si è riempito del 30%. Allora il demone bdflush scrive i dati sul disco. Se il buffer è pieno, i dati vengono scritti sul disco anche indipendentemente da kupdated una volta che il buffer si è riempito.

Avvertimento

Ripercusioni sulla sicurezza dei dati

Modificare le impostazioni del demone di aggiornamento del kernel (ingl. kernel update daemon) si ripercuote anche sulla sicurezza dei dati.

Avvertimento

Oltre a quanto descritto fin qui, anche i cosiddetti "Journaling File system", ad.es. ReiserFS o Ext3, scrivono indipendentemente da bdflush i loro metadati sul disco rigido, cosa che naturalmente "sveglia" continuamente il disco rigido. Per evitare ciò, vi è una estensione del kernel che è stata sviluppata appositamente per dispositivi mobili. La descrizione dettagliata la trovate in `/usr/src/linux/Documentation/laptop-mode.txt`.

Inoltre dovete anche considerare il comportamento dei programmi che state utilizzando. Per esempio buoni editor di testi scrivono "di nascosto" sul disco delle copie di sicurezza del file appena modificato. Queste funzionalità si lasciano comunque disabilitare, ma bisogna sempre tener conto della sicurezza dei dati.

In questo contesto vi è per il demone di posta elettronica postfix una variabile `POSTFIX_LAPTOP` che se impostata su `yes`, postfix riduce notevolmente il numero degli accessi al disco. Comunque ciò diventa trascurabile se l'intervallo per kupdated è stato esteso.

16.5 Il pacchetto powersave

Il pacchetto `powersave` è stato ideato appositamente per applicazioni che girano sui portatili, essendo preposto al risparmio energetico quando è la batteria ad alimentare il sistema. Alcune funzionalità sono comunque anche di interesse per comuni postazioni di lavoro e server (ad es.: suspend/standby, funzionalità bottone ACPI e disattivazione di dischi IDE).

Questo pacchetto include tutte le funzionalità di power management del vostro sistema. Esso supporta hardware che utilizza ACPI, APM, dischi IDE e la tecnologia PowerNow! o SpeedStep. Le funzionalità dei pacchetti `apmd`, `acpid`, `ospmd` e `cpufreqd` (adesso `cpuspeed`) vengono riunite nel pacchetto `powersave`. Per tale ragione non si dovrebbe lavorare parallelamente con demoni presi da questi pacchetti e il demone di powersave.

Anche se il vostro sistema non dispone di tutti gli elementi hardware summenzionati (APM e ACPI si escludono a vicenda), vale la pena utilizzare il demone

di powersave per regolare il risparmio energetico. Eventuali modifiche della configurazione dell'hardware vengono rilevate automaticamente dal demone.

Importante

Su powersave

Oltre al presente capitolo sono reperibili ulteriori informazioni sul pacchetto powersave anche sotto `/usr/share/doc/packages/powersave`.

Importante

16.5.1 Configurazione del pacchetto powersave

powersave si configura tramite diversi file:

`/etc/sysconfig/powersave/common`
Questo file serve al demone di powersave. Tra l'altro sussiste la possibilità di aumentare la quantità dei messaggi di debug (in `/var/log/messages`) tramite il valore assegnato alla variabile `POWERSAVE_DEBUG` .

`/etc/sysconfig/powersave/events`
Questo file è richiesto dal deamon di powersave per garantire l' elaborazione degli eventi di sistema (ingl. events) che si verificano. Ad un evento possono essere assegnate azioni esterne o azioni eseguite dal daemon. Si parla di azione esterna quando il daemon tenta di invocare un file eseguibile che risiede sotto `/usr/lib/powersave/scripts/`. Azioni interne predefinite sono:

- ignore
- throttle
- dethrottle
- suspend_to_disk
- suspend_to_ram
- standby
- do_suspend_to_disk
- do_suspend_to_ram
- do_standby

`throttle` riduce l'attività del processore nella misura stabilita tramite il valore specificato in `POWERSAVE_MAX_THROTTLING`. Questo valore dipende dallo schema utilizzato al momento. `dethrottle` riporta il processore a pieno regime. `suspend_to_disk`, `suspend_to_ram` e `standby` innescano la modalità di sospensione. Si consiglia di assegnare questi stati del sistema a determinati eventi del sistema.

Gli script per l'elaborazione degli eventi di sistema sono raccolti nella directory `/usr/lib/powersave/scripts`:

notify notifica il verificarsi di un evento tramite console, X window o segnale acustico

screen_saver abilitare il salvaschermo

switch_vt di aiuto se in seguito ad un suspend/standby la schermata risultasse discostata

wm_logout salvare le impostazioni ed eseguire il logout da GNOME, KDE o da un altro window manager

wm_shutdown salvare le impostazioni di GNOME o KDE ed eseguire lo shutdown (spegnimento) del sistema

Se ad esempio impostate la variabile `POWERSAVE_EVENT_GLOBAL_SUSPEND2DISK="prepare_suspend_to_disk do_suspend_to_disk"`, non appena l'utente dà il comando a powersaved di entrare nello stato di sospensione `Suspend to disk` vengono eseguite le due azioni o gli script nella sequenza indicata. Il daemon invoca lo script esterno `/usr/lib/powersave/scripts/prepare_suspend_to_disk`. Una volta che ciò è stato eseguito correttamente, il deamon esegue l'azione interna `do_suspend_to_disk` e, dopo che lo script abbia scaricato i relativi moduli e fermato i relativi servizi, il sistema entra nel modo di sospensione.

Una modifica apportata all'evento di un tasto (button) (Sleep) potrebbe assumere il seguente aspetto: `POWERSAVE_EVENT_BUTTON_SLEEP="notify suspend_to_disk"`. In questo caso l'utente viene informato dallo script esterno `notify` sull' evento di sospensione. In seguito viene generato l'evento `POWERSAVE_EVENT_GLOBAL_SUSPEND2DISK` a cui seguono le azioni descritte sopra che permettono di passare in tutta sicurezza nel modo di sospensione. Lo script `notify` si lascia modificare tramite la variabile `POWERSAVE_NOTIFY_METHOD` che trovate in `/etc/sysconfig/powersave/common`.

/etc/sysconfig/powersave/cpufreq
: Il file contiene delle variabili per l'ottimizzazione delle impostazioni relative alla frequenza dinamica della CPU.

/etc/sysconfig/powersave/battery
: Contiene i limiti della batteria e altre impostazioni specifiche della batteria.

/etc/sysconfig/powersave/sleep
: In questo file stabilite i moduli da scaricare ed i servizi da fermare prima di entrare nel modo per così dire di dormiveglia, ed i quali dovranno essere in seguito ricaricati e riavviati. Inoltre potete ritardare l'attivazione di questa modalità (per poter eventualmente salvare ancora dei file.) Le impostazioni di default riguardano in prima linea i moduli USB e PCMCIA. Se un evento di sospensione o di stand-by dovesse fallire, spesso la causa è dovuta a determinati moduli. Si veda la sezione 16.5.4 a pagina 325 per maggiori dettagli sul modo di identificare l'errore.

/etc/sysconfig/powersave/thermal
: Qui impostate gli aspetti concernenti raffreddamento e ventilazione. Per maggiori dettagli rimandiamo al file `/usr/share/doc/packages/powersave/README.thermal`.

/etc/sysconfig/powersave/scheme_*
: Si tratta dei diversi schemi, detti anche profili, che regolano il consumo energetico in base a determinati scenari di applicazione, di cui alcuni sono già preconfigurati e possono essere subito utilizzati senza la necessità di apportare delle modifiche. Comunque sussiste inoltre la possibilità di salvare anche propri profili.

16.5.2 Configurazione di APM ed ACPI

Suspend e Standby

I modi di attività ridotta sono disabilitati di default, visto che su alcuni sistemi non producono gli effetti desiderati. In linea di massima vi sono tre modi di dormiveglia ACPI e due di APM:

Suspend to Disk (ACPI S4, APM suspend)
: Salva l'intero contenuto della memoria sul disco rigido. Il sistema si spegne completamente e non consuma alcuna energia.

Suspend to RAM (ACPI S3, APM suspend)
Salva gli stati dei dispositivi nella RAM, solamente la RAM continua a consumare energia.

Standby (ACPI S1, APM standby) Spegne alcuni dispositivi (dipende dai rispettivi produttori)

Assicurate che siano settate le seguenti opzioni standard per la corretta interpretazione di eventi suspend/standby e resume nel file `/etc/sysconfig/powersave/events` (cosa che si ha di solito ad installazione avvenuta di 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"
```

Stati della batteria definiti dall'utente

Nel file `/etc/sysconfig/powersave/battery` potete stabilire tre valori (espressi in punti percentuali) riguardanti lo stato di caricamento della batteria che una volta raggiunti, il sistema emette degli avvertimenti e vengono eseguite determinate azioni.

```
POWERSAVED_BATTERY_WARNING=20
POWERSAVED_BATTERY_LOW=10
POWERSAVED_BATTERY_CRITICAL=5
```

Le azioni/gli script che verranno eseguiti non appena si scende sotto la soglia dei valori impostati vengono impostati nel file di configurazione `/etc/sysconfig/powersave/events`. Inoltre potete modificare le azioni standard dei button come descritto nella sezione 16.5.1 a pagina 320.

```
POWERSAVE_EVENT_BATTERY_NORMAL="ignore"
POWERSAVE_EVENT_BATTERY_WARNING="notify"
POWERSAVE_EVENT_BATTERY_LOW="notify"
POWERSAVE_EVENT_BATTERY_CRITICAL="wm_shutdown"
```

Adattare il consumo energetico alle diversi condizioni di esecuzione

Potete correlare il comportamento del sistema al tipo dell'alimentazione energetica. Il consumo energetico del sistema dovrebbe ridurrsi quando il sistema funziona a batteria. Ed inversamente la performance del sistema dovrebbe incrementare non appena il sistema è connesso nuovamente alla rete elettrica. In concreto potete influire sulla frequenza della CPU, sulla funzione di risparmio energetico dei dischi IDE e su una serie di parametri.

In `/etc/sysconfig/powersave/events` stabilite l'esecuzione di determinate azioni alla connessione o disconnessione del sistema dalla o alla rete elettrica. In `/etc/sysconfig/powersave/common` selezionate gli scenari (detti schemes):

```
POWERSAVE_AC_SCHEME="performance"
POWERSAVE_BATTERY_SCHEME="powersave"
```

Gli schemes vengono archiviati nei file sotto `/etc/sysconfig/powersave`. Il loro nome si compone di: `scheme_nome dello schema`. Nell'esempio ne riportiamo due: `scheme_performance` e `scheme_powersave`. Preconfigurati sono `performance`, `powersave` e `presentation` e `acoustic`. Tramite il modulo YaST per il power management (si veda la sezione 16.6 a pagina 328) potete elaborare in qualsiasi momento schemi esistenti, crearne di nuovi, cancellare quelli esistenti o correlarli agli stati di alimentazione energetica del sistema.

16.5.3 Ulteriori feature ACPI

Se utilizzate ACPI potete determinare la reazione del vostro sistema tramite i cosiddetti *tasti ACPI* (power, sleep, e lid open e lid abbassato). In `/etc/sysconfig/powersave/events` stabilite l'esecuzione di determinate azioni. Per maggiori dettagli in riferimento alle opzioni consulate questo file di configurazione.

POWERSAVE_EVENT_BUTTON_POWER="wm_shutdown"
: Se premete il tasto (Power) il sistema esegue lo shutdown del relativo window manager (KDE, GNOME, fvwm...).

POWERSAVE_EVENT_BUTTON_SLEEP="suspend_to_disk"
Se premete il tasto (Sleep) il sistema entra nel modo suspend to disk, ossia sospensione su disco.

POWERSAVE_EVENT_BUTTON_LID_OPEN="ignore"
Se alzate il display non succede niente.

POWERSAVE_EVENT_BUTTON_LID_CLOSED="screen_saver"
Se abbassate il display si attiva il salvaschermo.

Se il processore per un determinato lasso di tempo non raggiunge un determinato livello di attività, potete ridurre ulteriormente il livello di attività del processore. Impostate a riguardo tramite `POWERSAVED_CPU_LOW_LIMIT` e `POWERSAVED_CPU_IDLE_TIMEOUT` rispettivamente il livello minimo e l'intervallo di tempo una volta raggiunti o superati i quali si dovrà ridurre il livello di attività della CPU.

16.5.4 Troubleshooting

Date una occhiata a `/var/log/messages` in cui trovate protocollati i messaggi di errore e di allerta. Se scorrendo il file non individuate la causa del problema, istruite powersave nel file `/etc/sysconfig/powersave/common` tramite la variabile `DEBUG` di emettere dei messaggi più dettagliati. Impostate il valore della variabile su `7` o addirittura su `15` e riavviate il demone. Con messaggi più dettagliati in `/var/log/messages` alla mano dovrebbe essere possibile circoscrivere il problema. Tratteremo di seguito le difficoltà maggiormente riscontrate con powersave.

Non funzionano i tasti (ACPI abilitato con supporto hardware)

In caso di difficoltà dovute ad ACPI, analizzate da vicino l'output del comando `dmesg`, con particolare attenzione ai messaggi che riguardano ACPI, il comando è `dmesg|grep-i acpi`. A volte è necessario eseguire un aggiornamento del BIOS per risolvere la causa del problema. Visitate dunque il sito del produttore del portatile, scaricate ed installate una versione aggiornata del BIOS. Comunicate al produttore del vostro sistema di attenersi all'attuale specificazione dell' ACPI. Se gli errori persistono anche dopo l'aggiornamento del BIOS, sostiuite la DSDT contenente degli errori del vostro BIOS con una aggiornata:

1. Scaricate la DSDT adatta al vostro sistema da `http://acpi.sourceforge.net/dsdt/tables` . Assicuratevi che il file sia scompattato e compilato - riconoscibile dalla estensione di file `.aml` (ACPI Machine Language). In questo caso passate al punto 3.

2. Se la tabella scaricata ha l'estensione di file `.asl` (ACPI Source Language), dovrete compilarla tramite iasl dal pacchetto `pmtools`. Invocate `iasl -sa file.asl`. L'ultima versione di iasl (Intel ACPI Compiler) è inoltre reperibile al seguente indirizzo `http://developer.intel.com/technology/iapc/acpi/downloads.htm`.

3. Copiate il file `DSDT.aml` dove preferite (noi consigliamo `/etc/DSDT.aml`). Editate `/etc/sysconfig/kernel` ed adattate di conseguenza il percorso del vostro file DSDT. Lanciate `mkinitrd` (pacchetto `mkinitrd`). Ogni volta che disinstallate il kernel e utilizzate `mkinitrd` per creare un initrd, la DSDT adattata verrà integrata e caricata al boot del sistema.

CPU frequency non funziona

Sorgenti del kernel alla mano (`kernel-source`) controllate se il vostro processore viene supportato oppure se dovete utilizzare eventualmente un determinato modulo del kernel o una determinata opzione del modulo per attivare il controllo della frequenza della CPU. I dettagli sono reperibili sotto `/usr/src/linux/Documentation/cpu-freq/*`. Se è richiesto un determinato modulo o una determinata opzione, configuratelo/la nel file `/etc/sysconfig/powersave/cpufre` tramite le variabili `CPUFREQD_MODULE` e `CPUFREQD_MODULE_OPTS`.

suspend e standby non funzionano

Ecco le possibili cause da ricondursi al kernel che ostacolano su sistemi ACPI il modo suspend/standby:

- Sistemi con oltre 1 Gbyte di RAM al momento non supportano il modo suspend
- Sistemi multi-processori o sistemi con un processore P4 (con hyper threading) attualmente non supportano il modo suspend.

L'errore può essere anche dovuto ad una implementazione DSDT errata (BIOS). In questo caso installare una nuova DSDT.

Per sistemi ACPI e APM vale: non appena il sistema tenta di scaricare un modulo corrotto, il sistema si blocca e non entra nel modo suspend. Allo stesso risultato si arriva anche nel caso inverso ovvero l'evento suspend non viene innescato perché non vengono scaricati o fermati dei moduli o servizi. In entrambi i casi dovreste provare a individuare i moduli che causano il problema. Di aiuto sono i file di log creati dal daemon di powersave sotto `/var/log/sleepmode`. In caso di difficoltà spesso il tutto si lascia ricondurre ad un modulo da scaricare prima di entrare nel modo di sospensione o standby. Potete intervenire sulle impostazioni sotto `/etc/sysconfig/powersave/sleep`.

```
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=""
```

Se ricorrete al modo di sospensione e standby in ambienti di rete in continuo cambiamento o con file system montati da remoto (ad es. Samba, NIS e altri), si consiglia di utilizzare l'automounter per eseguirne il mount oppure di inserire i rispettivi servizi (ad es. `smbfs` o `nfs`) nelle variabili menzionate sopra. Se prima di un evento suspend/standby si accede ad un file system montato da remoto tramite un programma, il servizio non si lascia fermare correttamente ed il file system non funziona correttamente. Dopo il ripristino del sistema il file system risulta eventualmente essere corrotto e dovrà essere montato nuovamente.

Con ACPI, il demone di powersave non rileva i limiti della batteria

In ACPI, il sistema operativo può richiedere dal BIOS una comunicazione quando la batteria scende sotto un certo livello di carica. Il vantaggio di questo metodo consiste nel non dovere costantemente leggere lo stato della batteria, che tra l'altro inciderebbe sulle prestazioni del sistema. Comunque può darsi il caso che contrariamente a quanto comunicato dal BIOS in realtà non viene inviata nessuna comunicazione al sistema operativo anche se si scende sotto il livello minimo indicato. In questi casi impostate la variabile `POWERSAVED_FORCE_BATTERY_POLLING` in `/etc/sysconfig/powersave/battery` su `yes` per forzare la lettura dello stato della batteria.

16.6 Il modulo per il power management di YaST

Grazie al modulo di YaST per il power management potete eseguire tutte le impostazioni in tema di power management che sono state illustrate nelle sezioni precedenti. Dopo l'inizializzazione del modulo tramite il controllo di YaST ('Sistema' → 'Power management') appare la prima maschera del modulo (si veda la figura 16.1 in questa pagina).

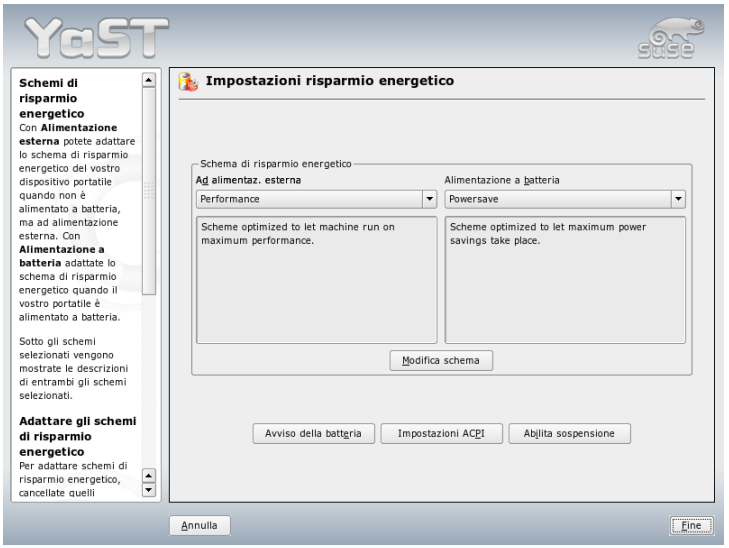

Figura 16.1: *Selezione schema*

In questa finestra potete selezionare lo schema da applicare in base alla alimentazione del vostro sistema, ovvero a batteria o tramite connessione alla rete elettrica. Se volete aggiungere o modificare gli schemi, cliccate su 'Modifica schemi' e avrete una rassegna degli schemi esistenti, si veda a riguardo anche la figura 16.2 a fronte.

Avete la possibilità di selezionare uno schema esistente tramite il menu a tendina oppure di visualizzare una panoramica degli schemi esistenti tramite il bottone 'Modifica'. Per creare uno schema nuovo cliccate su 'Aggiungi'. In entrambi

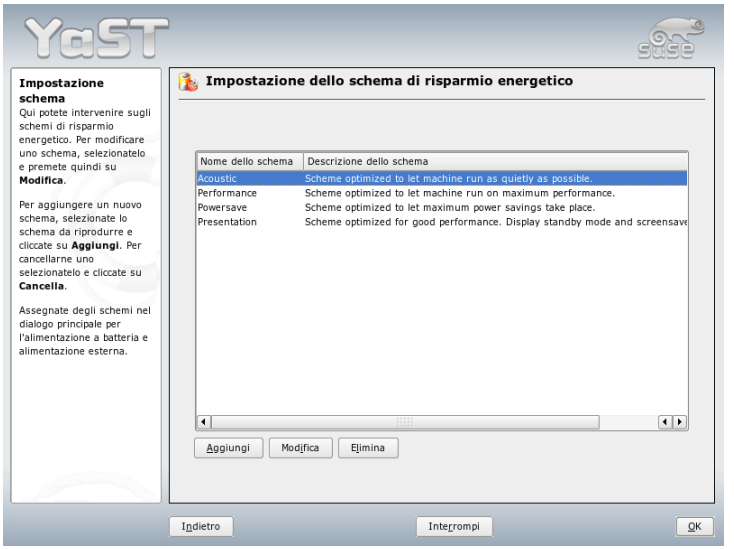

Figura 16.2: *Rassegna degli schemi esistenti*

i casi si giunge alla stessa finestra dialogo riportata nella figura 16.3 nella pagina successiva).

Assegnate come prima cosa allo schema nuovo o da modificare un nome (qualificante) ed una descrizione. Innanzitutto stabilite come e se si debba intervenire sulla performace della CPU per questo schema. Decidete se e fino a che punto si debba avere la 'Frequency scaling' ed il 'Throttling'. Nella finestra successiva stabilite una 'Strategia standby' per il disco rigido volta a realizzare il massimo in termini di prestazioni o in termini di risparmio energetico. La 'Strategia acustica' regola il livello di rumore del disco rigido (cosa che viene supportata purtroppo solo da pochi dischi IDE). La 'Strategia di raffreddamento' regola il tipo di raffreddamento da applicare. Purtroppo questa funzionalità viene supportata solo di rado dal BIOS. A riguardo rimandiamo a `/usr/share/doc/packages/powersave/README.thermal` per documentarvi sui metodi di raffreddamento passivo od il modo di utilizzare la ventola. Lasciate questa finestra cliccando nuovamente su 'OK' e le vostre impostazioni verranno applicate.

Nel dialogo iniziale potete eseguire anche delle impostazioni globali relative al power management, ossia consumo energetico. Cliccate su 'Avvertimenti batte-

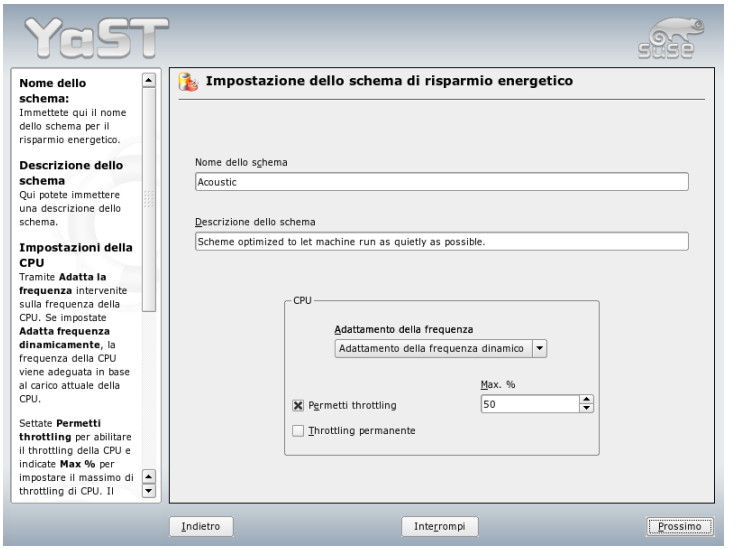

Figura 16.3: *Aggiungere uno schema*

ria', 'Impostazione ACPI' o 'Abilita sospensione'. Per giungere al dialogo sullo stato di caricamento della batteria, cliccate su 'Avvertimenti batteria' (si veda la figura 16.4 a fronte).

Non appena si scende sotto certi limiti configurabili, il BIOS lo comunica al vostro sistema operativo e potrete determinare quale tipo di reazione dovrà seguire come risposta. In questo dialogo stabilite il tetto massimo o il limite minimo per :'Livello di allerta', 'Livello basso' e 'Livello critico'. Nei primi due casi, il messaggio di allerta raggiunge direttamente l'utente, mentre se si scende sotto l'ultimo livello critico, il sistema sarà spento (shut down), visto che l'energia rimanente non basta a garantirne un funzionamento regolare. Selezionate gli stati di caricamento e la relativa azione in risposta confacente alle vostre esigenze e uscite dal dialogo con 'OK' per giungere nuovamente al dialogo iniziale.

Giungete alla finestra di configurazione dei pulsanti ACPI tramite 'Impostazioni ACPI' (si veda la figura 16.5 a pagina 332). Impostando i pulsanti ACPI stabilite il modo in cui debba reagire il sistema se si utilizzano determinati pulsanti. Questi pulsanti/eventi in ACPI si chiamano "Buttons". Configurate il tipo di risposta del sistema al premere del tasto (Power), del tasto (Sleep) ed all'abbassare del dis-

Figura 16.4: *Stato di caricamento della batteria*

play del portatile. Con 'OK' terminate la configurazione e ritornate al dialogo iniziale.

Tramite 'Abilita sospensione' giungete alla finestra in cui configurare se e come l'utente di questo sistema possa fare uso della funzionalità di suspend o stand-by. Fate clic su 'OK' per ritornare alla finestra principale. Uscite dal modulo premendo nuovamente su 'OK' per rendere effettive le vostre impostazioni che interessano il power management del vostro sistema.

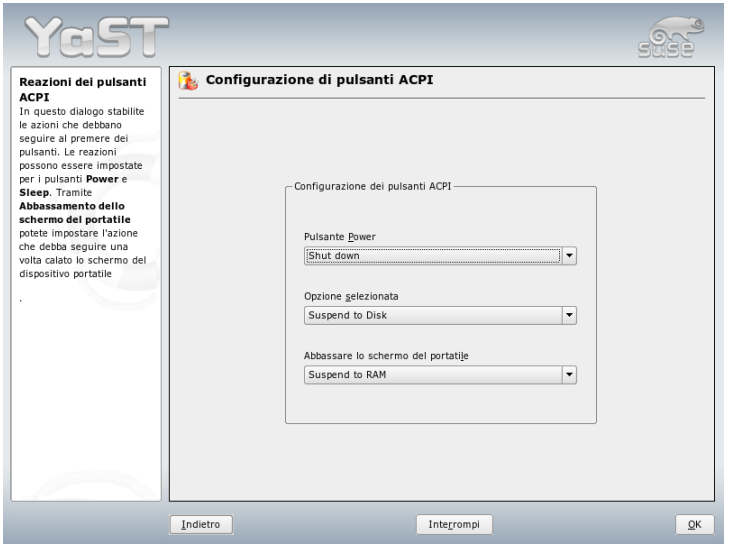

Figura 16.5: *Impostazioni ACPI*

Comunicazione wireless

Esistono diversi modi per fare comunicare il vostro sistema Linux con altri sistemi, periferiche o cellulari. Se volete collegare in rete dei notebook, selezionate WLAN (Wireless LAN). Bluetooth è in grado di connettere in rete singoli componenti di sistema (mouse, tastiera), periferiche, cellulari, PDA e singoli client. IrDA viene utilizzato in primo luogo per realizzare la comunicazione con PDA o cellulari. Questo capitolo illustrerà tutte e tre le tecnologie, configurazione compresa.

17.1 Wireless LAN

Le wireless LAN rappresentano ormai un aspetto indispensabile del computing mobile. Quasi tutti i notebook recenti hanno una scheda WLAN integrata. Lo standard delle schede WLAN è stato stabilito dall' organizzazione IEEE e si chiama 802.11. La velocità di trasmissione dei dati era originariamente di 2 MBit/s. Per incrementare tale tasso vi sono stati dei ritocchi in tema di modulazione, l'output di trasmissione e chiaramente la velocità di trasmissione.

Tabella 17.1: *Rassegna dei diversi standard WLAN*

Nome	Banda [GHz]	Velocità di trasmissione mass. [MBit/s]	Nota
802.11	2,4	2	obsoleto; non esistono praticamente più dei terminali
802.11b	2,4	11	molto diffuso
802.11a	5	54	meno diffuso
802.11g	2,4	54	compatibilità verso il basso con 11b

Vi sono inoltre degli standard proprietari come la variante 802.11b di Texas Instruments con un tasso di trasmissione massimo di 22 MBit/s (noto anche come 802.11b+). La diffusione di schede del genere è piuttosto esigua.

17.1.1 Hardware

SUSE LINUX non supporta schede 802.11, mentre supporta in linea di massima schede dello standard 802.11a, 802.11b, e 802.11g. Le schede recenti seguono il più delle volte lo standard 802.11g, ma vi sono ancora delle schede 802.11b sul mercato. Le schede con i seguenti chip vengono supportate:

- 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

Vengono supportate anche delle schede non proprio recenti, quasi non più reperibili sul mercato. Per un elenco esaustivo di schede WLAN con indicazione del chip utilizzato rimandiamo alle pagine di *AbsoluteValue Systems*: `http://www.linux-wlan.org/docs/wlan_adapters.html.gz` La seguente URL presenta una rassegna dei diversi chip WLAN: `http://wiki.uni-konstanz.de/wiki/bin/view/Wireless/ListeChipsatz`

Alcune schede richiedono un cosiddetto firmware image, che deve essere caricato nella scheda all'inizializzazione del driver, come è il caso per Intersil PrismGT, Atmel ACX100, ACX111. Potete installare il firmware in modo semplice ricorrendo a YOU (YaST Online Update). Il firmware per schede Intel PRO-Wireless è già contenuto in SUSE LINUX e verrà installato in modo automatico tramite YaST non appena viene rilevata una scheda del genere. Ulteriori informazioni sono reperibili una volta sistema installato sotto `/usr/share/doc/packages/wireless-tools/README.firmware`.

Scheda non supportate nativamente da Linux possono essere indirizzate eseguendo l'applicazione ndiswrapper. Questa applicazione utilizza driver Windows fornite assieme alla maggior parte delle schede WLAN. ndiswrapper viene descritto sotto `/usr/share/doc/packages/ndiswrapper/README.SUSE` (una volta installato il pacchetto `ndiswrapper`). Per degli approfondimenti rimandiamo al sito web del progetto: `http://ndiswrapper.sourceforge.net/support.html`.

17.1.2 Modo di funzionare

Tratteremo ora gli aspetti fondamentali di reti wireless. Illustreremo i vari modi operativi, metodi di autenticazione e di cifratura.

Modo operativo

In ambito di reti wireless si distingue fondamentalmente tra reti amministrate e reti ad hoc. Reti amministrate dispongono di un elemento principale, il cosiddetto access point, ovvero punto di accesso. In questa modalità (detta anche modalità infrastruttura) tutte le connessioni delle postazioni WLAN sulla rete avvengono tramite il punto di accesso, il quale permette di connettersi ad una ethernet.

Reti ad hoc non hanno un punto di accesso, le postazioni comunicano direttamente tra di loro. La portata ed il numero delle postazioni coinvolte sono nel caso di reti ad hoc molto limitati, quindi di solito si dà la preferenza a reti con punto di accesso. Sussiste addirittura la possibilità che una scheda WLAN funga da punto di accesso. Questa funzionalità supportata dalla maggioranza delle schede.

Dato che una rete wireless è più esposta a delle intercettazioni, e quindi più facile da compromettere rispetto ad una rete basata su cavi, i diversi standard prevedono dei metodi di l'autenticazione e cifratura. Nella versione originale dello standard IEEE 802.11 questi accorgimenti vengono designati tramite la sigla WEP. Dato che però WEP si è rilevato essere poco sicuro (si veda la sezione Sicurezza a pagina 341), l'industria WLAN (riunita sotto il nome *Wi-Fi Alliance*) ha definito una propria estensione dello standard, battezzandolo WPA che colma le lacune di WEP. Lo standard successivo 802.11i dell' IEEE (a volte denominato anche WPA2, WPA in fin dei conti scaturì da una versione di test di 802.11i) include WPA e dei metodi di autenticazione e cifratura.

Autenticazione

Nelle reti amministrate si ricorre ad una serie di meccanismi di autenticazione per assicurare che si loggano solo postazioni autorizzate:

Aperto In un sistema aperto non vi è autenticazione. Ogni postazione può entrare nella rete. Comunque si potrà ricorrere alla cifratura WEP (si veda la sezione Cifratura nella pagina successiva).

Chiave condivisa (secondo IEEE 802.11)
In questo procedimento viene utilizzata la chiave WEP ai fini dell'autenticazione. Comunque anche questa procedura è esposta a degli attacchi. Un potenziale aggressore dovrà solamente "osservare" per un lasso di tempo sufficiente il processo di comunicazione tra postazione e punto di accesso. Durante il processo di autenticazione i dati vengono scambiati una volta in modo cifrato ed una volta in modo non cifrato. Così la chiave utilizzata si lascierà dedurre facendo uso di determinati strumenti. E dato che con questa chiave WEP si effettua sia l'autenticazione che la cifratura, si intuisce subito che ciò non va ad incrementare il livello di sicurezza della rete. Una postazione in possesso della chiave WEP corretta è in grado di eseguire l'autenticazione come anche il processo di cifratura e decifratura. Un postazione sprovvista della chiave fallirà al momento di decifrare i pacchetti ricevuti. Quindi non potrà comunicare in modo corretto, a prescindere dal fatto se si debba autenticare o meno.

WPA-PSK (secondo EEE 802.1x) WPA-PSK (PSK sta per pre-shared key) funziona in modo simile al procedimento con chiave condivisa (ingl.shared key). Le postazioni interessate nonché il punto di accesso dispongono della stessa chiave, lunga 256 bit che di solito viene immessa sotto forma di frase segreta. Questo approccio rinuncia alla complessa amministrazione di chiavi come è invece il caso con WPA-EAP ed è indicato in prima linea per l'ambito domestico. Infatti, WPA-PSK a volte viene chiamato anche WPA "home".

WPA-EAP (secondo IEEE 802.1x) WPA-EAP in fondo non è un sistema di autenticazione, piuttosto si tratta di un protocollo per il trasporto delle informazioni richieste dal processo di autenticazione. Trova applicazione in ambito aziendale per tutelare reti wireless, mentre per le reti domestiche è quasi del tutto irrilevante. WPA-EAP viene dunque a volte chiamato anche WPA "enterprise".

Cifratura

I metodi di cifratura sono tesi ad assicurare che nessuno sprovvisto dell'autorizzazione possa leggere i pacchetti scambiati in una rete wireless o addirittura ottenere l'accesso alla rete:

WEP (definito nell' IEEE 802.11) Questo standard ricorre all'algoritmo di cifratura RC4, originariamente con una lunghezza chiave di 40 bit, successivamente anche di 104 bit. Spesso come lunghezza si indicano 64 o rispettivamente 128 bit, a seconda se si sommano o meno i 24 bit del cosiddetto vettore di inizializzazione. Questo standard presenta comunque dei punti deboli, vi sono anche dei modi di attaccare la chiave generata da questo sistema. Il ricorso a WEP resta comunque preferibile ad una rete completamente non protetta.

TKIP (definito nel WPA/IEEE 802.11i) Questo protocollo definito nello standard WPA per l'amministrazione delle chiavi utilizza lo stesso algoritmo di cifratura di WEP, elimandone comunque il punto debole. Per ogni pacchetto dati viene generata una nuova chiave, quindi sferrare degli attacchi contro le chiavi non frutta quasi nulla. TKIP viene utilizzato assieme a WPA-PSK.

CCMP (definito nell'IEEE 802.11i) CCMP è il metodo di amministrazione delle chiavi che di solito viene utilizzato assieme a WPA-EAP, e che comunque

può essere utilizzato anche con WPA-PSK. Per la cifratura si ricorre all'algoritmo AES che risulta più solido rispetto alla cifratura RC4 dello standard WEP.

17.1.3 Configurazione con YaST

Per configurare la schede di rete wireless, avviate il modulo 'Scheda di rete'. Nella finestra 'Configurazione dell'indirizzo di rete' selezionate il tipo di dispositivo 'Wireless' e fate clic su 'Prossimo'.

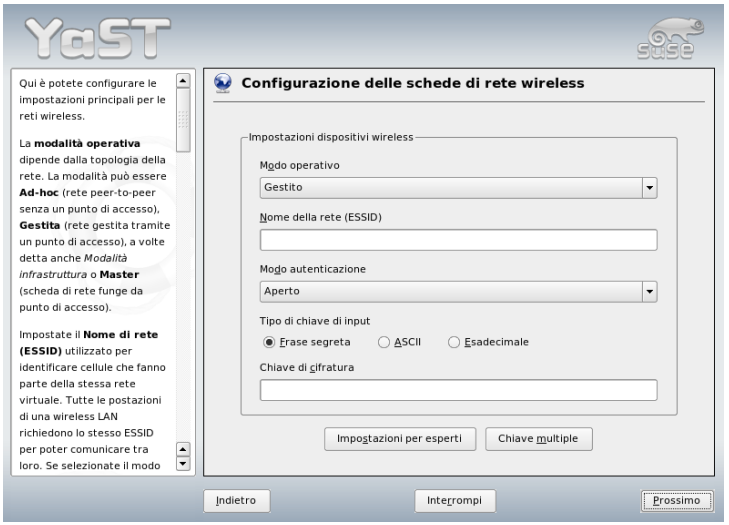

Figura 17.1: *YaST: configurazione della scheda di rete wireless*

Nel dialogo successivo 'Configurazione scheda di rete wireless' (si veda la figura 17.1 in questa pagina) eseguite le impostazioni di base in tema di WLAN:

Modo operativo Vi sono tre modi di integrare la vostra postazione in una WLAN. Il modo più congruo alle vostre esigenze dipende dalla struttura della rete all'interno della quale intendete scambiare dei dati: 'Ad-hoc' (rete prettamente peer-to-peer senza punto di accesso), 'Amministrata' (rete amministrata da un punto di accesso) e 'Master' (la vostra scheda di rete debba fungere da punto di accesso)

Nome rete (ESSID) Tutte le postazioni all'interno di una rete wireless richiedono lo stesso ESSID per poter scambiare dei dati. In assenza di un ESSID, la scheda tenterà automaticamente di rilevare un punto di accesso che potrà essere diverso da quello che intendevate utilizzare.

Modo d'autenticazione Selezionate un metodo di autenticazione appropriato alla vostra rete. Potrete scegliere tra: 'Aperto', 'Chiave condivisa' e 'WPA-PSK'. Se selezionate 'WPA-PSK', va impostato un nome di rete.

Per esperti Tramite questo bottone potrete eseguire le impostazioni dettagliate riferite al vostra connessione WLAN. La finestra verrà illustrata più avanti nel presente capitolo.

Dopo aver terminato l'impostazione di base, la vostra postazione potrà essere utilizzata in una WLAN.

Importante

Sicurezza in una rete wireless

Utilizzate in ogni caso uno dei metodi di autenticazione e cifratura supportati per tutelare la vostra rete. Connessioni WLAN non cifrate permettono a terzi di spiare in modo indisturbato i dati in transito sulla vostra rete. Anche un debole metodo di cifratura (WEP) è da preferire a nessuna cifratura. In caso di dubbio leggete la sezione Cifratura a pagina 337 e la sezione Sicurezza a pagina 341.

Importante

In base al metodo di cifratura selezionato, YaST vi chiederà in una delle finestre susseguenti di eseguire delle impostazioni mirate riferite al metodo selezionato. Per 'Aperto' non vi è nulla da impostare in aggiunta.

Chiavi WEP Selezionate il modo di immissione della chiave: 'Frase segreta', 'ASCII' o 'Esadec.'. Sono consentite fino a quattro chiave preposte alla cifratura dei dati trasmessi. Tramite 'Chiave multiple' entrate nella finestra di configurazione delle chiavi. Impostate la lunghezza delle chiavi, potete scegliere tra '128 bit' e '64 bit'. Di default si ha '128 bit'. Determinate quale debba essere la chiave di default tramite 'Imposta default'. La prima chiave viene considerata da YaST come chiave di default, se non ne marcate esplicitamente un'altra. Se cancellate la chiave di default, dovrete indicare manualmente quale chiave rimasta debba fungere da chiave di default. Tramite 'Modifica' potete intervenire su voci dell'elenco o generare una

nuova chiave, nel qual caso una finestra pop-up vi chiede di selezionare il tipo di immissione: 'Frase segreta' 'ASCII' o 'Esadec.'. Se selezionate 'Frase segreta' immettete un'espressione o una sequenza di caratteri da cui verrà generata la chiave in base alla lunghezza stabilita in precedenza. 'ASCII' richiede una immissione di cinque caratteri per chiavi lunghe 64 bit e di 13 caratteri per chiavi lunghe 128 bit. Se selezionate il modo di immissione 'Esadec.', dovete immettere 10 caratteri per chiavi di 64 bit e 26 caratteri per chiavi di 128 bit direttamente nell'annotazione esadecimale.

WPA-PSK Per una chiave WPA-PSK selezionate tra il metodo di immissione 'Frase segreta' o 'Esadec.'. Nel modo 'Frase segreta' l'immissione deve essere composta da otto fino a 63 caratteri; nel modo 'Esadec.' si hanno 64 caratteri.

Tramite 'Per esperti...' uscite dalla finestra per le impostazioni di base ed entrate in quella per esperti in tema di accesso WLAN. Ecco le opzioni a vostra disposizione:

Canale Dovrete stabilire un determinato canale per la vostra postazione WLAN solo nella modalità 'Ad-hoc' o 'Master'. Nella modalità 'Amministrata' la scheda cerca di rilevare automaticamente il punto di accesso nei canali disponibili. Nella modalità 'Ad-hoc' potete selezionare uno dei 12 canali disponibili per comunicare con le altre postazioni. Nella modalità 'Master' determinate su quale canale la vostra scheda debba fungere da punto di accesso. La preimpostazione di questa opzione è 'Auto'.

Bitrate Sempre in base alle prestazioni della vostra rete è consigliabile preimpostare un determinato bitrate per la trasmissione dei dati. Con l'impostazione di default 'Auto' il sistema cercherà di realizzare il trasferimento dei dati quanto velocemente possibile. Tenete presente che non tutte le schede WLAN consentono di impostare il bitrate.

Punto di accesso In un ambiente con diversi punti di accesso potete preselezionarne uno tramite l'indicazione dell'indirizzo MAC.

Usa power management Durante degli spostamenti si consiglia di prolungare la durata della batteria quanto possibile ricorrendo a delle tecniche di risparmio energetico. Per maggiori informazioni sul power management, ovvero funzionalità di risparmio energetico sotto Linux rimandiamo al capitolo 16 a pagina 307.

17.1.4 Tool utili

hostap (pacchetto `hostap`) viene utilizzato per impiegare una scheda WLAN come punto di accesso. Per maggiori informazioni su questo pacchetto andate sulla home page del progetto (`http://hostap.epitest.fi/`).

kismet (pacchetto `kismet`) è un tool con finalità diagnostiche per controllare il traffico di pacchetti WLAN e poter quindi rilevare in questo modo anche dei tentativi di intrusione nella vostra rete. Per maggiori informazioni si veda `http://www.kismetwireless.net/` o la rispettiva pagina di manuale.

17.1.5 Tips & Tricks: configurazione di una WLAN

Ecco cosa dovete sapere in tema di velocità, stabilità nonché sicurezza della vostra WLAN.

Stabilità e velocità

Il funzionamento affidabile e performante di una rete wireless dipende dal fatto se le postazioni coinvolte ottengono dei segnali ineccepibili dalle altre. Delle barriere tipo pareti domestiche chiaramente indeboliscono il segnale. Meno forte è il segnale e più lentamente verranno trasmessi i dati. Potete rilevare la potenza del segnale con il sistema in esecuzione ad esempio tramite il programma iwconfig dalla riga di comando (campo `Link Quality`, ossia qualità del collegamento) o tramite il programma di KDE kwifimanager. In caso di problemi da ricondurre alla qualità del segnale provate a cambiare locazione dei dispositivi o a cambiare la posizione delle antenne del vostro punto di accesso. Alcune schede PCMCIA-WLAN hanno delle antenne aggiuntive che migliorano notevolmente la qualità del segnale. La velocità indicata dai produttori (ad es. 54 MBit/s) è sempre da intendere come nominale. Si tratta del valore massimo teoreticamente possibile, nella prassi però il tasso (troughput) effettivo non è che la meta del valore nominale.

Sicurezza

Quando configurate una rete wireless dovete considerare che senza misure di sicurezza chiunque nei pressi potrà accedervi senza che sia richiesto un grande sforzo. Quindi si consiglia assolutamente di abilitare un metodo di cifratura. Tutte le schede WLAN o punti di accesso supportano la cifratura WEP. Non si

tratta di un protocollo del tutto blindato, ma comunque complica la vita a potenziali aggressori. In ambito domestico WEP è nella maggior parte dei casi sufficiente, anche se è preferibile utilizzare WPA-PSK che però non è implementato in punti di accesso non proprio recenti o router con funzionalità WLAN. A volte aggiornando il firmware si ottiene il supporto a WPA, approccio che purtroppo non produce il risultato desiderato sempre e comunque. Anche da parte di Linux, il supporto a WPA non è dato su ogni hardware. Al momento della stesura del presente capitolo, WPA viene supportato solo da schede con chip Atheros o Prism2/2.5/3, e in questo caso solo se si utilizza il driver hostap (si veda la sezione Difficoltà con schede Prism2 in questa pagina). Nei casi in cui non vi è supporto a WPA vale: meglio WEP che nessuna cifratura. In ambito aziendale, in cui vigono ben altri requisiti di sicurezza, una rete wireless andrebbe implementa esclusivamente con WPA.

17.1.6 Difficoltà possibili e possibili soluzioni

Se la vostra scheda WLAN non dovesse funzionare, assicuratevi di aver scaricato il firmware adatto e necessario. Si veda a riguardo anche la sezione 17.1.1 a pagina 334 all'inizio del capitolo.

Schede di rete multiple

Notebook recenti dispongono di solito di una schede di rete e di una scheda WLAN. Se avete configurato entrambi i dispositivi tramite DHCP (allocazione degli indirizzi automatica), eventualmente si possono verificare delle difficoltà con la risoluzione dei nomi e con il gateway di default. Questo tipo di problema si riconosce dal fatto che potete eseguire un ping indirizzato al router, ma non potete navigare su Internet. Vi è un articolo nella nostra banca di supporto dedicato a questo tema, eseguite semplicemente una ricerca usando la parola chiave "DHCP" su `http://portal.suse.com`.

Difficoltà con schede Prism2

Per dispositivi con chip Prism2 vi sono diversi driver di cui alcuni funzionano bene ed altri meno bene con le diverse schede. Con queste schede WPA è solo possibile con il driver hostap. Se si verificano delle difficoltà con queste schede, oppure se non funzionano o funzionano per così dire solo saltuariamente oppure se volete utilizzare WPA, siete pregati di leggere `/usr/share/doc/packages/wireless-tools/README.prism2`.

WPA

La presente versione di SUSE LINUX supporta WPA. Sotto Linux il supporto a WPA non può però dirsi maturo a tutti gli effetti. YaST infatti riesce a configurare solo WPA-PSK. WPA non funziona con alcune schede, altre richiedono un aggiornamento del firmware prima di poter utilizzare WPA. Se volete utilizzare WPA, consultate `/usr/share/doc/packages/wireless-tools/README.wpa`.

17.1.7 Ulteriori informazioni

Una vasta raccolta di informazioni utili in tema di reti wireless è reperibile sul sito Internet di Jean Tourrilhes, lo sviluppatore dei *wireless tool* per Linux: `http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html`

17.2 Bluetooth

Bluetooth è uno standard wireless per la connessione di una serie di dispositivi come cellulari, PDA, periferiche o componenti di sistema, ossia tastiera o mouse e notebook. Il nome deriva da un re danese di nome Blatand ("Harold Bluetooth" in inglese), il quale nel decimo secolo riuscì a rappacificare e riunire diverse fazioni scandinave belligerenanti. Il logo di Bluetooth si basa sulla runa "H" (che rassomiglia ad una stella) e "B".

Bluetooth si differenzia da IrDA, visto che i singoli dispositivi non devono "vedersi" direttamente e che i dispositivi possono costituire una rete. Comunque si ha un tetto massimo di 720 Kbps per la velocità di trasmissione dei dati (indicazione valida per la versione 1.2). In teoria Bluetooth consente una comunicazione tra dei dispositivi anche attraverso delle mura, ma molto dipende anche dallo spessore delle mura e dalla classe alla quale appartengono i dispositivi, vi sono tre classi che si distinguono in base alla loro portata massima che varia dai 10 fino ai 100 metri.

17.2.1 Concetti basiliari

Nelle seguenti sezioni verranno trattati i principi che stanno alla base del funzionamento di Bluetooth. Indicheremo i requisiti di software da soddisfare, il modo in cui Bluetooth interagisce con il vostro sistema ed faremo luce sui cosiddetti profili Bluetooth.

Software

Per poter utilizzare la tecnologia Bluetooth serve un adattatore Bluetooth (sia esso integrato nel dispositivo o un dongle esterno), dei driver e un cosiddetto "bluetooth protocol stack". Il kernel Linux include già una serie di driver per l'utilizzo di Bluetooth. Come "Protocol Stack" si ricorre al sistema Bluez. Affinché le diverse applicazioni possano funzionare con Bluetooth, vanno installati Inoltre i pacchetti di base (`bluez-libs`, e `bluez-utils` che mettono a disposizione una serie di servizi e programmi richiesti. Per alcuni adattatori (Broadcom, AVM BlueFritz!) è inoltre necessario installare `bluez-firmware`. Il pacchetto `bluez-cups` permette di stampare tramite una connessione Bluetooth.

Flusso di lavoro

Un sistema Bluetooth è composto da quattro strati connessi tra di loro che mettono a disposizione la funzionalità desiderata:

Hardware L'adattatore ed il driver adatto per il supporto da parte del kernel Linux.

File di configurazione La gestione del sistema Bluetooth.

Daemon Servizi gestiti tramite i file di configurazione che mettono a disposizione le diverse funzionalità.

Applicazioni Programmi che permettono di accedere e gestire le funzionalità messe a disposizione dal daemon.

Inserendo l'adattatore Bluetooth viene caricato il relativo driver dal sistema hotplug. Dopo che il driver è stato caricato, viene controllato in base al file di configurazione se va lanciato Bluetooth. In questo caso viene stabilito quali servizi debbano essere lanciati. In base a queste informazioni vengono avviati i rispettivi daemon. Adapter Bluetooth vengono rilevati subito dopo l' installazione. Se ne viene rilevato uno o più, Bluetooth viene abilitato. Altrimenti per motivi di sicurezza il sistema Bluetooth è disabilitato di default. Ogni dispositivo Bluetooth aggiunto successivamente va abilitato manualmente.

I profili

In Bluetooth i servizi vengono definiti in cosiddetti profili. Lo standard di Bluetooth prevede ad esempio dei profili per il transfer di dati (profilo "File Transfer"), la stampa (profilo "Basic Printing") e connessioni di rete (profilo "Personal

Area Network"). Affinché un dispositivo possa avvalersi di un servizio di un altro dispositivo, entrambi i dispositivi devono supportare il profilo in questione, un dato che spesso purtroppo non è deducibile né dalla confezione né dal rispettivo manuale del dispositivo. Inoltre vi sono dei produttori che seguono alla lettera le definizioni dei singoli profili ed altri meno. Di solito comunque ciò non si ripercuote sul processo di comunicazione tra i dispositivi.

In quello che segue partiamo dal presupposto che i dispositivi locali sono connessi fisicamente al sistema. Tutti gli altri dispositivi che possono essere indirizzati solo attraverso una connessione wireless vengono chiamati dispositivi remoti.

17.2.2 La configurazione

In questa sezione illustreremo la configurazione di Bluetooth. Ecco i file di configurazione interessati, i tool richiesti ed il modo di configurare Bluetooth tramite YaST o manualmente.

Configurazione Bluetooth tramiteYaST

Il modulo Bluetooth di YaST (si veda la figura 17.2 nella pagina seguente) permette di configurare il supporto a Bluetooth sul vostro sistema. Non appena il sistema hotplug rivela un adattatore Bluetooth nel vostro sistema, Bluetooth viene avviato automaticamente con le impostazioni qui stabilite.

Come prima cosa stabilite se sul vostro sistema debbano essere avviati i servizi Bluetooth. Se avete abilitato i servizi Bluetooth vanno configurate due cose. Innanzitutto, il 'Nome di dispositivo', che è il nome i dispositivi visualizzano quando viene rilevato il vostro sistema. Possono esservi due segnaposto—`%h` per il nome host del sistema (utile se ad esempio viene assegnato dinamicamente tramite DHCP) e `%d` per il numero dell'interfaccia (utile solo se disponete di più di un adattatore Bluetooth). Per fare un esempio, se immettete `Laptop %h` e DHCP assegna al vostro sistema il nome `unit123`, gli altri dispositivi remoti rilevano il vostro sistema come `Laptop unit123`

Il secondo parametro 'Security manager' si riferisce al modo di reagire del sistema locale quando un dispositivo remoto tenta di connettersi. Più precisamente al modo in cui viene gestito il codice PIN. Potete consentire a tutti i dispositivi di connettersi senza che sia richiesto un codice PIN o stabilire altrimenti il modo in cui selezionare il codice PIN corretto. Potete indicare un codice PIN (salvato in un file di configurazione) nell'apposito campo di immissione. Quando un dispositivo tenta di connettersi, utilizza questo PIN. Se l'esito è negativo prova senza PIN.

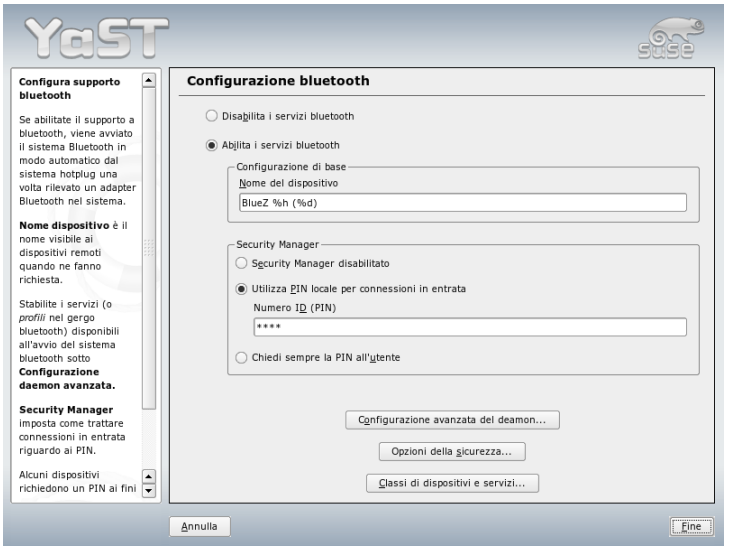

Figura 17.2: *YaST: configurazione Bluetooth*

Per il massimo in termini di sicurezza si consiglia di optare per la terza possibilità, “Chiedi sempre il PIN all’utente”. Questa opzione vi permette di utilizzare differenti PIN per differenti dispositivi (remoti).

Cliccate su ‘Configurazione avanzata del daemon’ per giungere nella finestra delle selezioni e configurazione dei servizi disponibili (in Bluetooth detti anche *profili*). Tutti i servizi disponibili vengono visualizzati in un elenco e possono essere accessi o spenti tramite ‘Abilitare’ o ‘Disabilitare’. Tramite ‘Modifica’ potete specificare ulteriori argomenti per il servizio selezionato (daemon). Apportate delle modifiche solo con cognizione di causa. Una volta conclusa la configurazione del daemon, uscite dal dialogo con ‘OK’

Ritornate nella finestra principale, dove per giungere nella finestra attinente agli aspetti di sicurezza e impostare cifratura, metodo di autenticazione e scansione dovete cliccare su ‘Opzioni della sicurezza’. Uscite dalla finestra per le impostazioni di sicurezza e ritornerete nella finestra principale. Dopo aver chiusa finestra principale con ‘Fine’, il vostro sistema Bluetooth è pronto per l’uso.

Dalla finestra principale giungete anche alla finestra ‘Classi di dispositivi e servizi’. I dispositivi Bluetooth sono raggruppati in vari “Classi di dispositivi”. In

questa finestra potete selezionare quella adatta al vostro sistema, ad es "Desktop" o "Laptop". La classe di dispositivi non ha un ruolo di primo piano, come è invece il caso per la "Classe di servizio", che potete impostare anche in questa sede. A volte dispositivi Bluetooth remoti come ad es. cellulari consentono di usufruire di certe funzionalità solo se rilevano la corretta classe di servizio. Ad esempio i cellulari si aspettano una classe chiamata "Object Transfer" prima di consentire il transfer di file dal o verso il vostro sistema. Avete modo di selezionare più classi. Comunque si sconsiglia di selezionare tutte le classi "per tutti i casi." La selezione di default di solito si rivela essere appropriata nella maggioranza dei casi

Per creare una rete tramite Bluetooth, abilitate nella finestra 'Configurazione avanzata daemon' 'PAND' e adattate, servendovi del bottone 'Modifica', il modo del daemon. Per una connessione di rete Bluetooth funzionante, un pand deve girare nel modo 'Listen' e la controparte nel modo 'Search'. Di default è preimpostato il modo 'Listen'. Adattate il comportamento del vostro pand locale. Configurate inoltre nel modulo YaST 'Scheda di rete' l'interfaccia `bnepX` (`X` sta per il numero di dispositivo nel sistema).

Configurazione manuale di Bluetooth

I file di configurazione per le singoli componenti del sistema Bluez si trovano nella directory `/etc/bluetooth`. L'unica eccezione si ha per il file preposto all'inizializzazione dei componenti `/etc/sysconfig/bluetooth` che viene modificato dal modulo YaST.

Solo `root` potrà modificare i file di configurazione riportati di seguito. Attualmente purtroppo non vi è un'interfaccia grafica tramite la quale poter intervenire su tutte le impostazioni. Potete comunque ricorrere al modulo Bluetooth di YaST per le principali impostazioni, come descritto nella sezione Configurazione Bluetooth tramiteYaST a pagina 345. Tutte le altre impostazioni sono di interesse solo per l'utente esperto per casi particolari. Di solito comunque le preimpostazioni sono sufficienti.

I codici PIN evitano che si creino delle connessioni indesiderate. Alla stregua del procedimento che conosciamo dalla telefonia mobile, i cellulari richiedono solitamente un codice PIN durante la prima presa di contatto (o meglio durante la configurazione sul cellulare della prima presa di contatto). Due dispositivi per poter scambiare dei dati tra di loro devono avere lo stesso PIN. Il codice PIN lo trovate sul sistema nel file `/etc/bluetooth/pin`.

Importante

Connessioni Bluetooth e la sicurezza

Nonostante i codici PIN, bisogna tenere presente che è possibile intercettare la comunicazione tra due dispositivi. Ed inoltre tenete presente che essendo disabilitate, bisogna prima abilitare l'autenticazione e cifratura di connessioni Bluetooth. Abilitare autenticazione e cifratura comporta eventualmente delle difficoltà nel processo di comunicazione con certi dispositivi Bluetooth.

Importante

Nel file di configurazione `/etc/bluetooth/hcid.conf` potete intervenire su diverse impostazioni come ad esempio il nome di dispositivo e la modalità di sicurezza. In linea di massima le impostazioni di default dovrebbero rilevarsi sufficienti. Il file contiene dei commenti che descrivono le opzioni delle singole impostazioni.

Nel file fornito a corredo vi sono due sezioni intitolate `options` e `device`. La prima contiene informazioni generali a cui ricorre hcid in fase di avvio. La seconda contiene le impostazioni per i singoli dispositivi Bluetooth locali.

Una della impostazioni più importanti nella sezione `options` è `security auto;`. Se si imposta `auto`, hcid tenta di utilizzare il PIN locale per connessioni in entrata. Se ciò non dovesse produrre l'esito atteso, prova con `none` creare la connessione in ogni modo. Per un più elevato livello di sicurezza si consiglia di impostare come default `user`, in modo che l'utente debba indicare ad ogni connessione il codice PIN.

Nella sezione `device` specificate il nome con cui il sistema viene visualizzato sulla controparte. Qui definite la classe dei dispositivi (`Desktop`, `Laptop` o `Server`) e abilitate o disabilitate l'autenticazione ed il metodo di cifratura.

17.2.3 Componenti del sistema e tool utili

Bluetooth si basa sulla combinazione di diversi servizi: sono richiesti almeno due demoni che girano in background (in sottofondo): hcid (*Host Controller Interface* che funge da interfaccia per il dispositivo e Bluetooth e permette gestirlo; sdpd (*Service Discovery Protocol* che comunica ai dispositivi i servizi offerti dal sistema. Sia hcid che sdpd possono essere inizializzati espicitamente con `rcbluetooth start` se ciò non dovesse avvenire automaticamente all'avvio del sistema. Il comando va eseguito come utente `root`.

Segue una breve descrizione dei principali tool di shell necessari per lavorare con Bluetooth. Anche se Bluetooth si lascia gestire tramite diverse componenti grafiche, si consiglia di dare almeno un'occhiata a questi programmi.

Alcuni comandi possono essere eseguiti solo da `root`, come ad es. `l2ping` ⟨*`indirizzodispositivo`*⟩, che vi permette di testare la connessione ad un dispositivo remoto.

hcitool

hcitool vi consente di stabilire se sono stati rilevati dispositivi locali o remoti. Con il comando `hcitool dev` saranno visualizzati dispositivi locali. L'output presenta una riga del tipo ⟨*nomeinterfaccia*⟩ ⟨*indirizzodispositivo*⟩ per ogni dispositivo locale rilevato.

Con `hcitool inq` potete rilevare dispositivi remoti. Verranno riprodotti tre valori per ogni dispositivo rilevato: l'indirizzo di dispositivo, differenza orario e classe di dispositivo. Di maggior interesse è l'indirizzo di dispositivo, perché viene utilizzato dagli altri comandi per identificare il dispositivo meta. La differenza orario è di interesse solo da un punto di vista prettamente tecnico. La classe specifica il tipo di dispositivo e di servizio sotto forma di valore esadecimale.

Tramite `hcitoolname` ⟨ *`indirizzodispositivo`*⟩ potete rilevare il nome di dispositivo di un dispositivo remoto. Se si tratta ad esempio di ulteriore client, la classe e il nome di dispositivo corrisponderanno ai dati riportati nel rispettivo `/etc/bluetooth/hcid.conf`. Indirizzi di dispositivi locali generano una comunicazione di errore.

hciconfig

Il comando `/sbin/hciconfig` emette ulteriori informazioni riguardanti il dispositivo locale. Invocando `hciconfig` senza nessun argomento vengono visualizzate delle informazioni sul dispositivo come nome di dispositivo `hciX`), indirizzo di dispositivo fisico (numero composto da 12 cifre tipo `00:12:34:56:78`) nonché delle informazioni sul volume dei dati trasmessi.

`hciconfig hci0 name` emette il nome che viene indicato dal vostro sistema quando riceve delle richieste da dispositivi remoti. `hciconfig` comunque non rileva solamente le impostazioni del dispositivo locale, ma permette anche di modificarle. Con `hciconfig hci0 name TEST` potete ad es. impostare il nome `TEST`.

sdptool

sdptool vi informa sul servizio offerto da un determinato dispositivo. `sdptool browse` ⟨*`indirizzodispositivo`*⟩ ritorna tutti i servizi del dispositivo, mentre con `sdptool search` ⟨*`codiceservizio`*⟩ si può cercare in modo mirato un determinato servizio. Con questo comando vengono interrogati tutti i dispositivi indirizzabili per quel che riguarda il servizio richiesto. Se un dispositivo mette a disposizione il servizio richiesto, il programma ritorna il nome completo ed una breve descrizione del dispositivo. Eseguendo `sdptool` senza alcun parametro si ottiene un elenco dei codici dei servizi.

17.2.4 Applicazioni grafiche

Se in Konqueror immettete l'URL `bluetooth:/` otterrete un elenco dei dispositivi Bluetooth locali e remoti. Eseguendo un doppio clic sul dispositivo avrete una rassegna dei servizi messi a disposizione dal dispositivo. Passate con il mouse su uno dei servizi elencati ed in basso nella finestra di stato del browser vedete quale profilo viene utilizzato per il servizio. Cliccate su un servizio e appare una finestra in cui vi verrà chiesto cosa intendete fare: salvare, utilizzare il servizio (a tal fine va lanciata una applicazione) o se interrompere l'operazione. Qui potete inoltre stabilire che questa finestra non dovrà più comparire, e che venga eseguita sempre l'operazione da voi selezionata. Tenete presente che per alcuni servizi non vi è (ancora) alcun supporto, per alcuni altri vanno eventualmente aggiunti dei pacchetti.

17.2.5 Esempi

In questa sezione riportiamo due esempi tipici riferiti alle possibilità di applicazione di Bluetooth. Nel primo verrà illustrato come creare una connessione di rete tra due host tramite Bluetooth e nel secondo viene illustrato come stabilire una connessione tra un computer ed un cellulare.

Collegamento via rete tra due host

Nel primo esempio vogliamo creare un collegamento di rete tra due host, *H1* e *H2* con indirizzo di dispositivo Bluetooth *baddr1* e *baddr2* che si lasciano rilevare come descritto sopra tramite `hcitool dev` su entrambi i sistemi. Gli host infine dovranno assumere l'indirizzo IP `192.168.1.3` (*H1*) e `192.168.1.4` (*H2*).

In Bluetooth la connessione si realizza tramite pand (*Personal Area Networking*). I comandi riportati di seguito devono essere eseguiti dall'utente `root`. Non entreremo nei dettagli per quel che riguarda i comandi di rete `ip`, ci concentreremo invece sulle operazioni che interessano da vicino Bluetooth.

Sull'host *H1* si lancia pand dando il comando `pand-s` . Sull' host *H2* con `pand -c` ⟨*baddr1*⟩ si può creare il collegamento. Se a questo punto invocate su uno degli host `ip link show` per avere un elenco delle interfacce di rete disponibili, si avrà un output del genere:

```
bnep0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
link/ether 00:12:34:56:89:90 brd ff:ff:ff:ff:ff:ff
```

Al posto di `00:12:34:56:89:90` vi sarà l'indirizzo del dispositivo locale (*baddr1* o *baddr2*). L'interfaccia va abilitata dopo averle assegnato un indirizzo IP. Per realizzare ciò su *H1* si immettono i seguenti due comandi

```
ip addr add 192.168.1.3/24 dev bnep0
ip link set bnep0 up
```

Su *H2* si immette:

```
ip addr add 192.168.1.4/24 dev bnep0
ip link set bnep0 up
```

Ora *H1* può essere contattato da *H2* tramite l'indirizzo IP `192.168.1.3`. Con `ssh 192.168.1.4` potete indirizzare *H2* da *H1* (sempre che su *H2* giri sshd, cosa che si ha di default in SUSE LINUX). Il comando `ssh 192.168.1.4` può essere immesso anche dall'utente "normale".

Transfer di dati dal cellulare al computer

Nel secondo esempio illustreremo come trasferire una foto scattata con un cellulare con camera digitale integrata (foto cellulare) - senza incorrere in costi aggiuntivi dovuti ad esempio all'invio di un mail multimediale - su un computer. Chiaramente il modo in cui sono strutturati i menu del cellulare varia da modello a modello, ma l'approccio da seguire non si discosta più di tanto. All'occorrenza consultate la guida del vostro cellulare. La descrizione qui riportata si riferisce ad una foto scattata con un Sony Ericsson da trasferire su un portatile. Per realizzare questo trasferimento sul portatile è richiesto il servizio Obex-Push ed inoltre il portatile dovrà consentire l'accesso al cellulare. Innanzitutto dobbiamo mettere a disposizione il servizio sul portatile, ricorrendo al demone opd dal pacchetto `bluez-utils`. Lanciatelo con:

```
opd --mode OBEX --channel 10 --daemonize --path /tmp --sdp
```

Due parametri sono quelli di rilievo. `--sdp` comunica il servizio a sdpd. Il parametro `--path /tmp` indica al programma dove memorizzare i dati ricevuti in questo caso abbiamo `/tmp`. Potete indicare anche un altro percorso però non dimenticate che dovete disporre dell'accesso in scrittura per la directory indicata.

Ora "presentate" il cellulare al portatile. Vi serve il menu 'Connessioni' del cellulare e selezionate lì 'Bluetooth'. Eventualmente andate su 'Attivare', prima di selezionare la voce 'Dispositivi propri'. Selezionate 'Nuovo dispositivo' e fate rilevare il portatile al vostro cellulare. Una volta rilevato, verrà visualizzato il suo nome sul display. Selezionate il dispositivo associato al portatile. A questo punto vi dovrebbe venir chiesto di indicare il codice PIN, immettete qui il codice PIN specificato in `/etc/bluetooth/pin`. Ora il vostro cellulare riconosce il portatile e può scambiare dei dati con esso. Uscite dal menu e cercate il menu per le immagini. Selezionate la foto da trasferire e premete su 'Ancora'. Nel menu che apparirà tramite 'Invia' potete selezionare il modo in cui inviare la foto. Selezionate 'Tramite Bluetooth'. A questo punto il portatile dovrebbe essere indirizzabile come dispositivo meta. Dopo aver selezionato il portatile avviene la trasmissione e la foto verrà archiviata nella directory specificata con il comando `opd`. Seguendo lo stesso approccio potreste anche trasferire un brano musicale sul vostro portatile.

17.2.6 Come risolvere possibili difficoltà

Se dovessero verificarsi dei problemi di connessione procedete come descritto di seguito. Ricordate sempre che la causa dell'errore può essere dovuta ad un dispositivo coinvolto nel processo di comunicazione e nel peggior dei casi, addirittura essere riconducibile ad entrambi le parti coinvolte nella connessione. Se possibile, cercate di eseguire delle verifiche con ulteriori dispositivi Bluetooth per escludere degli errori dovuti ai dispositivi:

Il dispositivo locale viene indicato nell'output di `hcitooldev`?
: Se il dispositivo locale non compare nell'output allora o l'hcid non è stato avviato o il dispositivo non viene riconosciuto come dispositivo Bluetooth. Ciò può verificarsi per ragioni diverse: il dispositivo è rotto, manca il giusto driver etc... . Nel caso di notebook con Bluetooth integrato vi è anche spesso un interruttore on/off per dispositivi wireless come WLAN e Bluetooth. Consultate il manuale di sistema del vostro notebook per vedere se il vostro dispositivo ha un interruttore del genere. Riavviate il sistema Bluetooth con

`rcbluetooth restart` e date una occhiata a `/var/log/messages` per vedere se si sono verificati degli errori.

Il vostro adattatore Bluetooth richiede un file firmware?
In questo caso installate `bluez-bluefw` e riavviate il sistema Bluetooth con `rcbluetooth restart`.

L'output di `hcitool inq` ritorna altri dispositivi?
Eseguite questo comando più volte, può darsi il caso che la connessione non funzioni perfettamente per motivi da ricondurre alla banda di frequenza di Bluetooth che viene utilizzata anche da altri dispositivi.

I codici PIN concordano? Controllate, se il codice PIN del computer (vd. `/etc/bluetooth/pin`) ed il PIN del dispositivo meta concordano.

Il dispositivo remoto "vede" il vostro sistema?
Provate a realizzare la connessione dal dispositivo remoto, verificate se il dispositivo vede il vostro sistema.

É possibile creare una connessione di rete (si veda l'esempio 1)?
Se il primo esempio non porta all'effetto desiderato (connessione di rete), la causa può essere dovuta a diverse ragioni: può darsi che uno dei due sistemi non supporti il protocollo ssh. Eseguite un test con: `ping 192.168.1.3` o `ping 192.168.1.4`. Se funziona, controllate se è in esecuzione sshd. Una altra causa per l'insorgere di difficoltà potrebbe essere il fatto che uno dei due dispositivi dispone di impostazioni di rete in conflitto con l' indirizzo IP (`192.168.1.X` nel nostro esempio). Provate semplicemente con altri indirizzi, ad es. `10.123.1.2` e `10.123.1.3`.

Il notebook compare come dispositivo meta (esempio 2). Il dispositivo mobile rileva il servizio Obex-Push sul portatile?
Andate nel menu 'Dispositivi propri' e selezionate il rispettivo dispositivo e visualizzate 'Elenco dei servizi'. Se manca (anche dopo aver aggiornato l'elenco) Obex-Push, allora il problema è da ricondurre all'opd sul portatile. L' opd è stato avviato? Avete l'accesso in scrittura per la directory indicata?

E' possibile avere un trasferimento nella direzione inversa?
Se avete installato il pacchetto `obexftp` alcuni dispositivi, vari modelli della Siemens e Sony Ericsson, vi consentono di eseguire il comando `obexftp-b` ⟨*`indirizzodispositivo`*⟩ `-B 10 -p` ⟨*`foto`*⟩. Consultate a riguardo la documentazione del pacchetto reperibile sotto `/usr/share/doc/packages/obexftp`.

17.2.7 Ulteriori informazioni

Per una valida rassegna delle diverse guide incentrate sull'utilizzo e configurazione di Bluetooth, visitate il seguente sito: `http://www.holtmann.org/linux/bluetooth/`. Altre fonti di informazione e guide:

- HOWTO ufficiale del Bluetooth protocol stack integrato nel kernel: `http://bluez.sourceforge.net/howto/index.html`
- Connessione con PalmOS PDA (inglese): `http://www.cs.ucl.ac.uk/staff/s.zachariadis/btpalmlinux.html`

17.3 Trasmissione a infrarossi dei dati

IrDA *Infrared Data Association* è uno standard industriale per la comunicazione wireless tramite i raggi a infrarossi. Oggi sono molti i portatili che permettono di comunicare, basandosi sullo standard IrDA, per esempio con stampanti, modem, LAN o altri portatili. La trasmissione avviene in un intervallo tra 2400 bps e 4 Mbps.

IrDA ha due modi operativi. Nella modalità standard SIR, la porta a infrarossi viene indirizzata tramite una interfaccia seriale. Questa modalità funziona su quasi tutti i dispositivi. La modalità più veloce FIR necessita di un driver speciale per il chip IrDA. Comunque non vi è un driver appropriato per ogni tipo di chip. Inoltre va impostata la modalità desiderata nel BIOS setup del computer. Lì si vede anche quale interfaccia seriale viene utilizzata per la modalità SIR.

Ulteriori informazioni su IrDA si trovano nell'IrDA-Howto di Werner Heuser sotto `http://tuxmobil.org/Infrared-HOWTO/Infrared-HOWTO.html` e sulla home page del Linux IrDA Project: `http://irda.sourceforge.net/`

17.3.1 Software

I moduli del kernel necessari sono contenuti nel pacchetto del kernel. Il pacchetto `irda` mette a disposizione le utility necessarie al supporto della porta ad infrarossi. Dopo aver installato il pacchetto, trovate la documentazione sotto `/usr/share/doc/packages/irda/README`.

17.3.2 Configurazione

Il servizio di sistema IrDA non viene avviato automaticamente al boot. Usate il modulo IrDA di YaST ai fini dell'abilitazione che presenta solo una impostazione da poter modificare: l'interfaccia seriale del dispositivo a infrarossi. Nella finestra di test vi sono due output. Una volta quello del programma `irdadump` che protocolla tutti i pacchetti IrDA inviati e ricevuti. In questo output dovrebbe essere indicato il nome del sistema ed il nome di tutti i dispositivi a infrarossi che si trovano nei suoi pressi. Un esempio per questo tipo di messaggio è reperibile nella sezione 17.3.4 nella pagina seguente. Tutti i dispositivi connessi tramite IrDA vengono elencati nella parte inferiore della finestra.

Purtroppo il consumo energetico (alimentazione a batteria) di IrDA è elevato, poichè a intervalli di pochissimi secondi viene inviato un pacchetto cosiddetto discovery per il rilevamento automatico di altri dispositivi periferici. Così si consiglia, soprattutto se è la batteria ad alimentare il sistema, di avviare IrDA solo in caso di necessità; con il comando `rcirda start` attivate l'interfaccia manualmente e con `rcirda stop` la disabilitate. Quando attivate l'interfaccia, tutti i moduli del kernel necessari vengono caricati automaticamente.

La configurazione manuale va eseguita nel file `/etc/sysconfig/irda` dove trovate una variabile `IRDA_PORT` con la quale determinare quale interfaccia debba venire usata nella modalità SIR.

17.3.3 Uso

Se volete stampare servendovi dei raggi infrarossi, potete inviare i dati tramite il file di dispositivo `/dev/irlpt0`. Il file di dispositivo `/dev/irlpt0` si comporta come l'interfaccia connessa via cavo `/dev/lp0`, con la sola differenza che i dati da stampare vengono inviati in modo wireless tramite i raggi ad infrarossi. Quanto stampate, tenete presente che la stampante deve essere visibile per l'interfaccia a infrarossi del sistema e che venga avviato il supporto per la funzionalità a infrarossi.

Una stampante che viene usata tramite una porta ad infrarossi, si lascia configurare tramite YaST. Visto che la stampante non viene rilevata automaticamente, iniziate il processo di configurazione con 'Altre (non rilevate)'. Nel prossimo dialogo potete selezionare 'Stampante IrDA'. Come collegamento `irlpt0` va quasi sempre bene. Per dei dettagli che riguardano il processo di stampa sotto Linux rimandiamo al capitolo 12 a pagina 249.

Se volete comunicare tramite la porta ad infrarossi con altri computer, con telefonini o dispositivi simili, potete farlo con il file di dispositivo `/dev/ircomm0`.

Con il telefonino S25 della Siemens per esempio potete collegarvi, tramite l'interfaccia a infrarossi, senza aver bisogno dei cavi ovvero wireless, ad Internet tramite il programma wvdial. Potete anche sincronizzare i vostri dati con un Palm Pilot, basta immettere nel rispettivo programma `/dev/ircomm0` come dispositivo.

Tenete presente che potete indirizzare solo dispositivi che supportano i protocolli della stampante o IrCOMM. Grazie a programmi particolari come irobexpalm e irobexreceive, potete indirizzare anche dispositivi che utilizzano il protocollo IROBEX (3Com Palm Pilot). Maggiori dettagli sono reperibili nell'*IR-HOWTO* (`http://tldp.org/HOWTO/Infrared-HOWTO/`). I protocolli supportati dal dispositivo vengono indicati nella parentesi quadra dopo il nome del dispositivi nell'output di `irdadump`. Il supporto al protocollo IrLAN si trova in fase di sviluppo.

17.3.4 Troubleshooting

Se i dispositivi alla porta ad infrarossi non dovessero reagire, controllate come `root`, con il comando `irdadump` se vengono rilevati altri dispositivi dal computer. Nel caso di una stampante Canon BJC-80 nei pressi del computer si ha un output simile al seguente ripetuto più volte (cfr. l'esempio 17.1 in questa pagina.

Esempio 17.1: *Output di 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=* terra
                        hint=0500 [ PnP Computer ] (21)
```

Se non si ha alcun output o l'altro dispositivo non risponde, controllate la configurazione della porta. State utilizzando la porta giusta? A volte la porta ad infrarossi si trova anche sotto `/dev/ttyS2` o `/dev/ttyS3`, o state usando un interrupt diverso da IRQ 3. Queste impostazioni si lasciano configurare su quasi ogni portatile nel BIOS setup.

Con una semplice videocamera potete anche controllare se si accende il LED a infrarossi - a differenza dell'occhio umano la maggior parte delle videocamere riesce a captare i raggi infrarossi.

Il sistema hotplug

Il sistema hotplug controlla l'inizializzazione della maggior parte di dispositivi di un computer. Tale sistema non viene utilizzato solo per dispositivi che possono essere inseriti e rimossi con il sistema in esecuzione, ma che per tutti i dispositivi rilevati al boot del sistema. L'hotplug si appoggia al file system `sysfs` ed a `udev` che viene illustrato in capitolo 19 a pagina 367.

Finché non viene caricato il kernel, vengono inizializzati solo dispositivi assolutamente necessari, tipo il bus system, dischi di boot e tastiera. Il kernel genera degli eventi hotplug per i dispositivi rilevati. Il demone `udevd` raccoglie questi eventi ed invoca i rispettivi script hotplug per poter inizializzare i dispositivi in questione. Nel caso di dispositivi che non possono essere rilevati automaticamente vi è il coldplug che replica eventi registrati o cerca nel sistema dei dispositivi non inizializzati e utilizza configurazioni statiche per dispositivi di vecchio stampo, come ISA.

Fatta eccezione per un numero ristretto di dispositivi, la maggiore parte dei dispositivi viene inizializzata al boot o al momento della connessione. Al processo di inizializzazione segue spesso la registrazione dell'interfaccia. Registrando l'interfaccia vengono innescati a sua volta degli eventi hotplug che comportano una configurazione automatica dell'interfaccia in questione.

Mentre in passato si partiva da un set di dati di configurazione applicando i quali si inizializzavano dei dispositivi; oggi si procede in modo esattamente inverso, ovvero si parte dai dispositivi presenti e si cercano i dati di configurazione adatti o si generano. Questo approccio consente di maneggiare in modo più flessibile i dispositivi hotplug.

Le principali funzionalità hotplug vengono configurate tramite due file: in `/etc/sysconfig/hotplug` trovate le variabili che determinano il comportamento di `hotplug` e `coldplug`. Ogni variabile viene illustrata da un commento. Il file `/proc/sys/kernel/hotplug` contiene il nome del programma eseguibile che viene invocato dal kernel. Le configurazione dei dispositivi sono reperibili sotto `/etc/sysconfig/hardware`. Con SUSE LINUX 9.3, questo file è vuoto, poiché `udevd` riceve dei messaggi hotplug tramite un netlink socket.

18.1 Dispositivi e interfacce

Il sistema hotplug non amministra solo dispositivi, ma anche le interfaccia; un dispositivo è connesso o al bus o ad una interfaccia. Il bus può essere considerato in tal senso un'interfaccia multipla. Oltre a dispositivi fisici vi sono anche dispositivi virtuali (ad es. tunnel di rete). Vi sono anche dispositivi virtuali, come tunnel di rete. I dispositivi di solito richiedono dei driver, sotto forma di moduli del kernel. Le interfacce vengono rappresentata dai nodi di dispositivo generati da `udev`. Distinguere tra dispositivi e interfacce è cruciale per meglio comprendere il concetto in sé.

I dispositivi registrati in `sysfs` sono riportati sotto `/sys/devices`, le interfacce si trovano sotto `/sys/class` o `/sys/block`. Tutte le interfacce del file `sysfs`

dovrebbero avere un riferimento (*ingl. link*) che punta sul rispettivo dispositivo, tuttavia vi sono ancora dei driver che non creano questo riferimento in modo automatico. Se manca il riferimento, non si sa a quale a dispositivo appartiene l'interfaccia e quindi non si riesce a trovare una configurazione adatta.

I dispositivi vengono indirizzati tramite una descrizione del dispositivo. Può trattarsi della "devicepath" in `sysfs` (`/sys/devices/pci0000:00/0000:00:1e.0/0000:02:00.0`) la descrizione del punto di connessione (`bus-pci-0000:02:00.0`), un proprio ID (`id-32311AE03FB82538`) o qualcosa di simile. Le interfaccia finora venivano indirizzate tramite il loro nome. Questo nome è in fin dei conti solo un numero nella sequenza dei dispositivi presenti e quindi possono cambiare se si aggiunge un dispositivo o se ne si rimuove uno.

Quindi anche le interfacce possono essere indirizzate tramite la descrizione del rispettivo dispositivo. Di solito è il contesto a chiarire se si intende la descrizione del dispositivo o la rispettiva interfaccia. Ecco degli esempi tipici per dispositivi, interfacce e rispettiva descrizione:

Scheda di rete PCI Un dispositivo connesso al bus PCI (`/sys/devices/pci0000:00/0000:00:1e.0/0000:02:00.0` o `bus-pci-0000:02:00.0`) e che dispone di una interfaccia di rete (`eth0`, `id-00:0d:60:7f:0b:22` o `bus-pci-0000:02:00.0`). L'interfaccia viene utilizzata dai servizi di rete o è connessa a dispositivi di rete virtuali come tunnel o VLAN, che a sua volta ha una propria interfaccia.

Controller SCSI PCI Un dispositivo (`/sys/devices/pci0000:20/0000:20:01.1/host1/1:0:0:0` o `bus-scsi-1:0:0:0`) che mette a disposizione diverse interfacce fisiche sotto forma di un bus (`/sys/class/scsi_host/host1`).

Dischi rigidi SCSI Un dispositivo (`/sys/devices/pci0000:20/0000:20:01.1/host1/1:0:0:0`) con diverse interfacce (`/sys/block/sda*`).

18.2 Eventi hotplug

Per ogni dispositivo e ogni interfaccia vi è un cosiddetto evento hotplug che viene elaborato dal rispettivo cosiddetto agente hotplug. Eventi hotplug vengono innescati o dal kernel non appena si crea una connessione ad un dispositivo o non appena il driver registra una interfaccia. A partire da SUSE LINUX 9.3, `udevd` riceve e distribuisce eventi hotplug. Vi sono due casi: `udevd` raccoglie direttamente messaggi netlink dal kernel oppure in `/proc/sys/kernel/`

hotplug va specificato /sbin/udevsend. Dopo che udevd assolto il suo compito (si veda il capitolo 19 a pagina 367), cerca un agente hotplug agent in /etc/hotplug.d/ corrispondente all'evento.

18.3 Agenti hotplug

Un agente hotplug non è altro che un programma eseguibile che esegue le operazioni adatte all'evento. Gli agenti per eventi dei dispositivi si trovano sotto /etc/hotplug⟨*nome evento* ⟩. Tutti i programmi in queste directory con il suffisso .hotplug vengono eseguiti in ordine alfabetico.

Per ignorare un determinato evento, rimuovete i bit di esecuzione dal rispettivo agente hotplug oppure cambiate il suffisso .hotplug a vostro piacimento.

Gli agenti dei dispositivi caricano soprattutto dei moduli del kernel, ma spesso devono invocare dei comandi aggiuntivi. Sotto SUSE LINUX questo compito viene assolto da /sbin/hwup o /sbin/hwdown. Questi programmi eseguono una ricerca di una configurazione appropriata al dispositivo nella directory /etc/sysconfig/hardware. Se un determinato dispositivo non deve essere inizializzato, allora va creato un file di configurazione adatto con il modo di avvio manual o off. Nel caso in cui /sbin/hwup non trova alcuna configurazione appropriata vengono caricati automaticamente dei moduli. In tal caso alcuni agenti generano automaticamente dei file di configurazione per hwup. In tal modo l'agente impiega meno tempo al prossimo volta che viene lanciato. Per maggiori dettagli rimandiamo alla sezione 18.4 a pagina 364. Informazioni su /sbin/hwup sono reperibili nel file /usr/share/doc/packages/sysconfig/README e nella pagina di manuale dihwup.

Agenti di interfacce vengono invocati in modo indiretto tramite udev, così udev creare nodo di dispositivo udev consente di assegnare dei nomi persistenti alle interfacce. Per maggiori dettagli rimandiamo al capitolo 19 a pagina 367. I singoli agenti configurano infine le interfacce. Segue una descrizione di alcune interfacce.

18.3.1 Attivare interfacce di rete

Interfacce di rete vengono inizializzate con /sbin/ifup e disattivate con /sbin/ifdown. Per maggiori dettagli rimandiamo al file /usr/share/doc/packages/sysconfig/README e alla pagina di manuale di ifup.

Se un sistema dispone di vari dispositivi di rete con driver diversi, può succedere che i nomi delle interfacce cambiano dopo il processo di boot, se questa volta è

stato caricato prima un driver diverso. Per questo motivo in SUSE LINUX gli eventi per dispositivi di rete PCI vengono amministrati tramite delle code. Potete sopprimere tale comportamento nel file `/etc/sysconfig/hotplug` tramite la variabile `HOTPLUG_PCI_QUEUE_NIC_EVENTS=no`.

La via maestra per avere dei nomi di interfacce consistenti è quella di indicare nei file di configurazione delle singole interfacce il nome desiderato. Per maggiori dettagli a riguardo rimandiamo al file `/usr/share/doc/packages/sysconfig/README`. Con SUSE LINUX 9.3, udev gestisce anche interfacce di rete, anche se non si tratta di nodi di dispositivo. Ciò consente di avere dei nomi di interfaccia persistenti.

18.3.2 Abilitare dispositivi di memorizzazione

Il mount delle interfacce dei dispositivi di memorizzazione può avvenire in modo del tutto automatico oppure venire preconfigurato. La configurazione avviene in `/etc/sysconfig/hotplug` tramite le variabili `HOTPLUG_DO_MOUNT`, `HOTPLUG_MOUNT_TYPE`, `HOTPLUG_MOUNT_SYNC` e nel file `/etc/fstab`. Il processo del tutto automatico viene abilitato impostando la variabile `HOTPLUG_DO_MOUNT=yes`. Vengono supportati due modi, potete passare dall'uno all'altro tramite la variabile `HOTPLUG_MOUNT_TYPE`.

Nel modo `HOTPLUG_MOUNT_TYPE=subfs` viene creata una directory nella directory `/media`, il cui nome si deduce dalle proprietà del dispositivo. Questo è il punto di mount automatico assegnatoli da `submountd` ogni volta che si accede al dispositivo. I dati in questo caso, i dati vengono scritti immediatamente, quindi in questa modalità potete rimuovere i dispositivi non appena si spegne il led luminoso per il controllo degli accessi. Nella modalità `HOTPLUG_MOUNT_TYPE=fstab` i dispositivi di memorizzazione vengono montati nel modo tradizionale in base alla registrazione nel file `/etc/fstab`.

Tramite la variabile `HOTPLUG_MOUNT_SYNC` potete selezionare se l'accesso debba avvenire nel modo sincrono o asincrono. Nel modo asincrono si ha un più rapido accesso in scrittura, visto che i risultati vengono bufferizzati; comunque può accadere che i dati non possano essere scritti in modo completo se si rimuove in modo repentino il supporto dati. Nel modo sincrono tutti i dati vengono immediatamente scritti e quindi l'accesso è più lento. Il processo di unmount, ovvero smontaggio, del dispositivo deve avvenire manualemente tramite `umount`.

Negli ultimi due modi operativi si consiglia l'utilizzo di nomi di dispositivi persistenti, dato che i nomi di dispositivo tradizionali possono cambiare a seconda della sequenza di inizializzazione. Per maggiori dettagli sui nomi di dispositivo persistenti rimandiamo al capitolo 19 a pagina 367.

18.4 Caricamento automatico di moduli

Se il tentativo di inizializzazione di un dispositivo tramite `/sbin/hwup` fallisce, l'agente cerca nella cosiddette *module map* un driver adatto. La preferenza viene data alle map di `/etc/hotplug/*.handmap` e se non trova nulla, prosegue con la ricerca in `/lib/modules/<versione_del_kernel>/modules.*map`. Se volete utilizzare un driver diverso da quello standard del kernel, indicatelo in `/etc/hotplug/*.handmap`, dato che questo file viene letto come primo.

Considerate le seguenti differenze tra USB e PCI. L'agente USB include nella sua ricerca di driver user mode anche i file `/etc/hotplug/usb.usermap` e `/etc/hotplug/usb/*.usermap`. Driver user mode sono dei programmi che regolano l'accesso al dispositivo al posto di un modulo del kernel. In questo modo è possibile invocare dei programmi eseguibili per determinati dispositivi.

Nel caso di dispositivi PCI `pci.agent` esegue una ricerca dei moduli driver in `hwinfo`. Se qui non trova nulla, l'agente prosegue nella sua ricerca includendo `pci.handmap` e la kernelmap, cosa però che è già stata fatta precedenza da `hwinfo` e che quindi produce nuovamente un esito negativo. `hwinfo` dispone di una banca dati aggiuntiva per la mappatura dei driver, che legge comunque anche `pci.handmap` per assicurare che in questo file venga applicata effettivamente una mappatura individuale.

Potete limitare la ricerca eseguita dall'agente `pci.agent` ad un determinato tipo di dispositivo o moduli driver di una determinata sottodirectory di `/lib/modules/<versione_del_kernel>/kernel/drivers`. Nel primo caso potete indicare le classi dei dispositivi, reperibili alla fine del file `/usr/share/pci.ids`, nel file `/etc/sysconfig/hotplug` tramite le variabili `HOTPLUG_PCI_CLASSES_WHITELIST` e `HOTPLUG_PCI_CLASSES_BLACKLIST`. Nel secondo caso specificate una o diverse directory nelle variabili `HOTPLUG_PCI_DRIVERTYPE_WHITELIST` e . `HOTPLUG_PCI_DRIVERTYPE_BLACKLIST`. I moduli che risiedono nelle directory escluse non verranno mai caricati. In entrambi i casi una whitelist vuota indica che tutte le possibilità sono ammesse tranne quelle specificate nella blacklist. Indicate nel file `/etc/hotplug/blacklist` i moduli che non dovranno essere mai caricati da un agente. Scrivete a riguardo ogni nome di modulo in un rigo a sé stante.

Se in un file mappa vengono rilevati una serie di moduli adatti viene caricato solo il primo modulo. Se desiderate che vengano caricati tutti i moduli dovete impostare la variabile `HOTPLUG_LOAD_MULTIPLE_MODULES=yes`. É comunque preferibile creare una propria configurazione del dispositivo `/etc/sysconfig/hardware/hwcfg-*` per il dispositivo in questione.

Ciò non vale per i moduli che vengono caricati tramite `hwup`. I moduli ven-

gono caricati in modo automatico solo in casi eccezionali ed il numero dei casi consentiti verrà ulteriormente ridotto nelle future edizioni di SUSE LINUX.

18.5 Hotplug con PCI

Alcuni sistemi supportano anche l'hotplug per dispositivi PCI. Per poter sfruttare questa possibilità vanno caricati dei particolari moduli del kernel che possono danneggiare sistemi che non supportano l'hotplug di dispositivi PCI. Gli slot per l'hotplug dei dispositivi PCI purtroppo non vengono rilevati automaticamente, quindi non resta che configurare questa funzionalità manualmente. Impostate a tal fine la variabile `HOTPLUG_DO_REAL_PCI_HOTPLUG`nel file `/etc/sysconfig/hotplug` su `yes`.

18.6 Script di boot coldplug e hotplug

`boot.coldplug` gestisce tutti i dispositivi non rilevati automaticamente, cioé per i quali non vi sono degli eventi hotplug. In questo caso viene invocato semplicemente `hwup` per ogni configurazione di dispositivo statica `/etc/sysconfig/hardware/hwcfg-static-*`. Si può ricorrere a questo meccanismo anche per inizializzare dispositivi integrati in una sequenza diversa rispetto a quella hotplug, visto che `coldplug` viene eseguito prima di `hotplug`.

`boot.hotplug` abilita l'elaborazione di eventi hotplug. Tramite il parametro di boot `khelper_max=0` vi è la consegna di eventi hotplug nella fase iniziale del processo di boot. Gli eventi già generati non vanno persi ma raccolti in una coda del kernel. Nel file `/etc/sysconfig/hotplug`, `boot.hotplug` stabilisce quanti eventi possono essere elaborati contemporaneamente, per assicurare una elaborazione corretta di tutti gli eventi.

18.7 Il debug

18.7.1 File protocollo

Di default `hotplug` protocolla in `syslog` solo pochi messaggi cruciali. Per avere delle informazioni più dettagliate va settata la variabile `HOTPLUG_DEBUG` nel file `/etc/sysconfig/hotplug` su `yes`. Se impostate questa variabile su `max` verrà protocollato ogni comando di shell di ogni script hotplug. Chiaramente si

avrà un /var/log/messages dalla notevoli dimensioni visto che syslog vi memorizza tutti i messaggi. Visto che durante il processo di boot syslog viene avviato dopo hotplug e coldplug i primissimi messaggi non potranno essere protocollati. Se si tratta di messaggi importanti per voi, impostate tramite la variabile HOTPLUG_SYSLOG un altro file di protocollo. Leggete a riguardo i commenti contenuti in /etc/sysconfig/hotplug.

18.7.2 Difficoltà al boot

Se un sistema va in panne durante il processo di boot potete disabilitare hotplug o coldplug immettendo al prompt di boot NOHOTPLUG=yes o rispettivamente NOCOLDPLUG=yes. Disabilitando il sistema hotplug, il kernel semplicemente non emette più eventi hotplug. Potrete riattivare il sistema hotplug una volta caricato il sistema eseguendo il comando /etc/init.d/boot.hotplug start . In questo caso verranno emessi ed elaborati tutti gli eventi hotplug generati fino a questo punto. Per scartare gli eventi in coda, inserite prima /bin/true in /proc/sys/kernel/hotplug dopo un po' ripristinare /sbin/hotplug. Disabilitando coldplug non vengono applicate le configurazioni statiche. Con /etc/init.d/boot.coldplug start riabilitate il sistema coldplug.

Per stabilire se è un determinato modulo caricato da hotplug ad essere la causa del problema, immettete al prompt di boot HOTPLUG_TRACE=<N>. Allo schermo verranno indicati l'uno dopo l'altro i nomi di tutti i moduli prima che vengono caricati effettivamente dopo $\langle N \rangle$ secondi. Qui non potete intervenire in modo interattivo.

18.7.3 Il registratore degli eventi

Lo script /sbin/hotplugeventrecorder viene invocato ad ogni evento da /sbin/hotplug e sbin/hotplug-stopped. Se vi è una directory /events, tutti gli eventi hotplug vengono archiviati sotto forma di singolo file in questa directory. Ciò vi dà modo di creare nuovamente un evento esattamente identico per eseguire dei test. Se non vi è una tale directory, gli eventi non vengono archiviati.

Nodi di dispositivo dinamici grazie a udev

Con il Linux Kernel 2.6 vi è una nuova soluzione *user space*, ovvero spazio utente, e cioé una directory di dispositivi dinamica `/dev` con nomi di dispositivi persistenti: `udev`. Indica solo i file dei dispositivi effettivamente presenti. Crea o rimuove i file per i nodi di dispositi che di solito risiedono sotto la directory `/dev` e rinomina le interfacce di rete. L'implementazione precedente di `/dev` con `devfs` non funziona più ed è stata sostituita da `udev`.

In passato nei sistemi Linux i cosiddetti *device node*, ovvero nodi di dispositivo, venivano archiviati nella directory `/dev`. Per ogni tipo di dispositivo vi era un nodo, indipendentemente dalla presenza effettiva del dispositivo. Di conseguenza la directory aveva una notevole dimensione. Il comando `devfs` apportò un notevole miglioramento su questo fronte, poiché solo dispositivi effettivamente esistenti presentavano un nodo di dispositivo in `/dev`.

`udev` percorre nuove vie nella creazione dei nodi di dispositivi: ricorrendo a delle regole confronta le informazioni che fornisce `sysfs` con le indicazioni dell'utente. `sysfs` è un nuovo file system del Kernel 2.6 e fornisce le informazioni basilari sui dispositivi connessi al sistema. `sysfs` viene montato sotto `/sys`.

L'utente non è tenuto a stabilire delle regole. Alla connessione del dispositivo viene creato il relativo nodo di dispositivo. Le regole permettono comunque di modificare il nome del nodo, cosa che si rileva essere utile nel caso di nomi di dispositivo di una certa complessità che in tal modo possono essere sostituiti con un nome intuitivo ed inoltre, se si connettono due dispositivi dello stesso tipo, si potranno assegnare dei nomi di dispositivo persistenti.

Se si dispone di due stampanti solitamente esse vengono designate con `/dev/lp0` e `/dev/lp1`; il nodo di dispositivo assegnato al dispositivo dipende dalla sequenza nella quale vengono accese le stampanti. Un altro esempio è rappresentato da dispositivi esterni di memoria di massa come ad esempio dischi rigidi USB. `udev` consente di registrare i percorsi esatti dei dispositivi in `/etc/fstab`.

19.1 Come impostare delle regole

`udev` legge i file sotto `/etc/udev/rules.d` con il suffisso `.rules` in ordine alfabetico prima di generare i nodi di dispositivo sotto `/dev`. Se vi sono diverse regole applicabili, viene applicata quella rilevata come prima. I commenti vengono introdotti da un #. Di solito le regole seguono la sintassi riportata:

```
key, [key,...] NAME [, SYMLINK]
```

Deve venir indicata almeno una chiave, visto che è tramite la chiave che viene assegnata una regola al dispositivo. Anche il nome è assolutamente necessario, dato che il nodo di dispositivo generato in `/dev` avrà questo nome. Il parametro facoltativo symlink consente di generare dei nodi anche altrove. A titolo di esempio riportiamo una regola per una stampante:

```
BUS="usb", SYSFS{serial}="12345", NAME="lp_hp", SYMLINK="printers/hp"
```

Questo esempio riporta due chiavi:BUS e SYSFS{serial}. udev compara il numero seriale con quello del dispositivo connesso al bus USB. Tutte le chiavi devono concordare per poter assegnare al dispositivo il nome lp_hp nella directory /dev. Inoltre verrà generato un link simbolico /dev/printers/hp che rimanda al nodo di dispositivo. La directory printers verrà generata automaticamente. Gli incarichi di stampa possono essere a questo punto inviati a /dev/printers/hp oppure a /dev/lp_hp.

19.2 Automatizzare NAME e SYMLINK

I parametri NAME e SYMLINK consentono di utilizzare degli operatori per automatizzare il processo di allocazione. Questi operatori fanno riferimento ai dati del kernel sul dispositivo in questione. Ecco un esempio a scopo illustrativo:

```
BUS="usb", SYSFS{vendor}="abc", SYSFS{model}="xyz", NAME="camera%n"
```

L'operatore %n viene sostituito con il numero del dispositivo della camera fotografica: camera0, camera1, etc. Un altro operatore utile è %k che viene sostituito dal nome di dispositivo standard del kernel, ad esempio hda1. Nelle regole udev potete anche invocare un programma esterno e utilizzare la stringa di ritorno per NAME e SYMLINK. Nella pagina di manuale di udev è reperibile un elenco di tutti gli operatori.

19.3 Espressioni regolari nelle chiavi

Le chiavi permettono l'uso di caratteri particolari, come le cosiddette wildcard nella shell. Il carattere * ad es. può essere utilizzato come segnaposto per dei caratteri e ? come segnaposto per esattamente un carattere.

```
KERNEL="ts*", NAME="input/%k"
```

Con questa regola viene assegnato ad un dispositivo il cui nome inizia con le lettere "ts" il nome kernel standard nella directory standard. Per delle indicazioni dettagliate che riguardano l'utilizzo delle espressioni regolari in tema di regole udev si rimanda alla pagina di manuale udev (man udev).

19.4 Selezione delle chiavi

Scegliere una chiave appropriata è il presupposto per una regola udev efficace. Delle chiavi standard sono ad esempio:

BUS Tipo di bus del dispositivo

KERNEL Nome di dispositivo del kernel

ID Numero di dispositivo connesso al bus (per es. ID del bus PCI)

PLACE Il punto effettivo ovvero dove il dispositivo è connesso (ad es. USB)

SYSFS{...} Attributi del dispositivo sysfs come etichetta, produttore, numero seriale, etc.

Le chiavi `ID` e `PLACE` possono rilevarsi utili, comunque nella maggioranza dei casi vengono utilizzate le chiavi `BUS`, `KERNEL` e `SYSFS{...}`. In aggiunta `udev` prevede l'utilizzo di chiavi che invocano script esterni e ne elaborano il risultato. Per informazioni dettagliate consultate la pagina di manuale di udev (`man udev`).

`sysfs` archivia dei piccoli file contenenti informazioni sull' hardware in un albero directory. Di solito un file contiene solo una informazione, sia essa il nome del dispositivo, il produttore o il numero di serie. Questi file possono essere utilizzati come valore della chiave. Se volete utilizzare diverse chiavi SYSFS{...} in una regola, potete utilizzare solo file che risiedono nella stessa directory. Il tool `udevinfo` vi aiuta a rilevare valori utili per chiavi.

Bisogna individuare sotto `/sys` una directory che si riferisce al rispettivo dispositivo e che contenga un file `dev`. Queste directory si trovano tutte sotto `/sys/block` o `/sys/class`. `udevinfo` si può rilevare utile anche se esiste già un nodo di dispositivo per il dispositivo. Il comando `udevinfo -q path -n /dev/sda` emette `/block/sda`, il che significa che la directory cercata è `/sys/block/sda`. Invocate quindi `udevinfo` con il seguente comando `udevinfo -a -p /sys/block/sda`. Potete anche combinare i due comandi: `udevinfo -a -p ‘udevinfo -q path -n /dev/sda‘`. Ecco un estratto dell'output del 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"
```

Dall'intero output e dall'abbondanza di informazioni, selezionate le chiavi appropriate che non cambieranno. Non dimenticate che per quanto riguarda le regole non potete utilizzare chiavi che risiedono in directory diverse.

19.5 Nomi consistenti per dispositivi di memoria di massa

SUSE LINUX contiene degli script che vi permettono di assegnare dei nomi consistenti per dispositivi di archiviazione come dischi rigidi e altri dispositivi simili, indipendentemente dalla sequenza in cui vengono inizializzati. `/sbin/udev.get_persistent_device_name.sh` è uno script wrapper che invoca innazitutto `/sbin/udev.get_unique_hardware_path.sh` per far rivelare il percorso hardware di un dato dispositivo. Inoltre `/sbin/udev.get_unique_drive_id.sh` rivela il numero di serie. Entrambi gli output vengono passati a `udev` che genera il link simbolico verso il nodo di dispositivo sotto `/dev`. Lo script wrapper può essere utilizzato direttamente nelle regole udev. Segue un esempio per dispositivi SCSI, applicabile anche a quelli USB o IDE (da inserire in un solo rigo):

```
BUS="scsi", PROGRAM="/sbin/udev.get_persistent_device_name.sh",
NAME="%k" SYMLINK="%c{1+}"
```

Non appena viene caricato un driver per un dispositivo di memoria di massa, esso registra tutti i dischi rigidi disponibili con il kernel, ognuno dei quali innescherà un evento hotplug block che invoca `udev`. `udev` in un primo tempo legge le regole per determinare se va generato un link simbolico o meno.

Se il driver viene caricato tramite il file `initrd` gli eventi hotplug andranno persi. Tutte le informazioni vengono comunque salvate in `sysfs`. L'utility

`udevstart` rileva tutti i file di dispositivo sotto `/sys/block` e `/sys/class` e quindi lancia `udev`.

In aggiunta vi è uno script di avvio `boot.udev` che genera ex novo tutti i nodi di dispositivo durante la fase di boot. Lo script di avvio va però attivato tramite l'editor dei runlevel di YaST oppure tramite il comando `insserv boot.udev`.

Suggerimento

Vi è tutta una serie di strumenti e programmi che fanno affidamento sul fatto che nel caso di `/dev/sda` si abbia un disco rigido SCSI e nel caso di `/dev/hda` un disco IDE. In caso contrario, i programmi non funzionano correttamente. YaST deve fare affidamento su questi strumenti e utilizza per tale ragione esclusivamente i nomi di dispositivo del kernel.

Suggerimento

File system di Linux

Linux supporta tutta una serie di file system. Questo capitolo vi offre una breve rassegna dei file system più noti sotto Linux. Illustreremo i concetti che stanno alla base, i rispettivi vantaggi e il loro campo di impiego preferenziale. Inoltre vi daremo qualche informazione sul "Large File Support" sotto Linux.

20.1 Glossario

Meta-dati La struttura interna del file system assicura un certo ordine e la disponibilità dei dati sul disco rigido. In un certo senso si tratta di "dati su altri dati". Quasi ogni file system ha una propria struttura di meta-dati. La differenza in termini di funzionalità dei singoli file system è da ricercare in questo ambito. E' estremamente importante mantenere intatti i meta-dati, altrimenti potrebbe andare distrutto l'intero file system.

Inode Gli inode contengono tutte le possibili informazioni sui file: nome, dimensione, numero dei link, data, orario di generazione, modifiche, diritti di accesso e puntatori (ingl.pointer) su blocchi del disco rigido su cui risiede il file.

Journal Nel contesto dei file system, il cosiddetto journal è una struttura interna del disco con una specie di protocollo in cui il driver del file system registra i (meta)dati del file system da modificare. Il "journaling" riduce notevolmente il tempo necessario per ripristinare un sistema Linux, poiché il driver del file system non deve cercare i meta-dati andati distrutti su tutto il disco, gli basta invece rileggere le registrazioni del journal.

20.2 I principali file system di Linux

La situazione è cambiata rispetto a due o tre anni fa', oggi non si ha solo la scelta tra Ext2 o ReiserFS. A partire dalla versione 2.4 il kernel offre una vasta scelta di file system. Segue una breve rassegna della modalità di funzionamento dei file system e dei loro vantaggi.

Chiaramente nessun file system si adatta perfettamente a tutte le applicazioni. Ogni file system ha dei vantaggi e dei svantaggi che vanno ponderati. Neanche il file system più sofisticato potrà mai sostituire un buon concetto di backup.

I termini *integrità dei dati* o *consistenza dei dati* in questo capitolo non si riferiscono alla consistenza dei dati memorizzati di un utente (quei dati che la vostra applicazione scrive nei vostri file). La consistenza dei dati deve essere garantita dalla stessa applicazione.

Importante

Configurare i file system

In tema di creazione e configurazione nonché partizionamento di file system si lascia realizzare tutto comodamente con YaST se non vengono indicati esplicitamente degli altri modi per apportare delle modifiche ai file system.

Importante

20.2.1 ReiserFS

Una delle funzionalità principali del kernel versione 2.4, ReiserFS, era disponibile a partire da SUSE LINUX 6.4 sotto forma di kernel patch per il SUSE kernel 2.2.x. ReiserFS è stato concepito da Hans Reiser e dall'équipe di sviluppatori Namesys. ReiserFS è una valida alternativa a Ext2. I suoi maggiori punti di forza sono una migliore gestione della memoria del disco rigido, migliore accessibilità al disco e ripristino veloce dopo un crollo del sistema.

Ecco i punti di forza di ReiserFS:

Miglior gestione della memoria del disco rigido
In ReiserFS i dati vengono organizzati in un struttura ad albero bilanciato (ingl. B*-balanced tree). La struttura ad albero contribuisce a sfruttare meglio la memoria del disco rigido, dato che piccoli file possono essere memorizzati nello stesso blocco, invece di essere memorizzati altrove e dover gestire il puntatore sulla localizzazione effettiva. Inoltre la memoria non viene assegnata nella misura di unità di 1 o 4 kbyte, ma esattamente nella misura richiesta. Un altro vantaggio è l'allocazione dinamica degli inode che rende i file system più flessibili rispetto ai tradizionali file system come ad esempio Ext2, dove bisogna indicare la densità degli inode al momento della generazione del file system.

Miglior accessibilità del disco rigido Nel caso di piccoli file vi sarete accorti che sia i dati file sia le informazioni (inode) "stat_data" vengono memorizzati gli uni accanto agli altri sul disco rigido. Basta accedere una volta sola al disco per avere tutte le informazioni di cui avete bisogno.

Ripristino veloce dopo un crollo del sistema
L'uso dei journal, per ricostruire le modifiche apportate ai meta-dati, riduce i tempi di verifica anche nel caso di grandi file system ad una manciata di secondi.

Affidabilità grazie al data Journaling ReiserFS supporta inoltre il data journaling e ed il data odered è simile a quanto illustrato nella sezione 20.2.3 a fronte dedicata a Ext3. Il modo di default è `data=ordered`, il quale assicura l'integrità sia dei dati che dei metadata, utilizzando comunque il journaling solo per i metadata.

20.2.2 Ext2

Ext2 risale agli inizi di Linux. Deriva dall'Extended File System ed è stato implementato nell'aprile del 1992 e dunque integrato in Linux 0.96c. L'Extended File System è stato successivamente modificato più volte e come Ext2 è stato per anni il più noto file system di Linux. Con l'avvento dei cosiddetti journaling file system e la velocità con la quale eseguono un ripristino, Ext2 perse in termini di importanza.

Forse una breve rassegna dei vantaggi di Ext2 vi aiuterà a capire come mai continua ad avere tanti sostenitori tra gli utenti Linux che ancora oggi preferiscono lavorare con questo file system.

Stabilità L'appellativo "solido come una roccia" non è dovuta al caso visto che nel corso degli anni Ext2 è stato continuamente migliorato ed ampiamente testato. Nel caso di un crollo del sistema senza un corretto smontaggio del file system, e2fsck analizza i dati del file system. I meta-dati vengono portati in una stato consistente, e file o blocchi di dati in sospeso vengono scritti in una determinata directory (chiamata `lost+found`). Contrariamente alla maggior parte dei journaling file system, e2fsck analizza l'intero file system e non solo i bit dei meta-dati modificati di recente. Questo richiede più tempo rispetto alla verifica dei dati protocollo di un journaling file system. A seconda del volume del file system, questo processo può durare mezz'ora o oltre. Per questo motivo Ext2 non è particolarmente adatto per server ad alta disponibilità. Dato che Ext2 comunque non deve aggiornare continuamente alcun journal e richiede una quantità notevolmente inferiore di memoria a volte risulta essere più veloce di altri file system.

Upgrade facile Basato sulla solida base di Ext2, Ext3 divenne l'acclamato file system di prossima generazione. L'affidabilità e la stabilità vennero coniugate sapientemente con i vantaggi di un journaling file system.

20.2.3 Ext3

Ext3 è stato sviluppato da Stephen Tweedie. Diversamente dai file system di "prossima generazione" Ext3 non si ispira a principi del tutto nuovi, si basa invece su Ext2. I due file system sono molto simili tra di loro; è semplice implementare un file system Ext3 su di un file system Ext2. La differenza principale tra Ext2 e Ext3 è che Ext3 supporta il journaling. Riassumendo, sono tre i vantaggi che offre Ext3:

Upgrade semplice ed estremamente affidabile da Ext2
Visto che Ext3 si basa sul codice di Ext2 e che appoggia sia il formato on-disk che il formato meta-dati di Ext2, gli upgrade da Ext2 verso Ext3 risultano essere facilissimi da eseguire. Si può eseguire un upgrade anche quando ad essere montati sono i file system di Ext2. Diversamente dalla migrazione verso altri journaling file system, come ReiserFS, JFS o XFS che può diventare una faccenda davvero laboriosa, (dovete fare delle copie di sicurezza di tutto il file system e successivamente ricostruirlo "ex novo"), passare a Ext3 è una questione di pochi minuti. Inoltre è molto sicuro visto che durante la ricostruzione di un completo file system spesso si possono verificare degli errori. Se si considera l'elevato numero di sistemi Ext2 che aspettano un upgrade a un journaling file system, si può facilmente intuire l'importanza di Ext3 per tanti sistemisti. Eseguire un downgrade da Ext3 a Ext2 è così facile come eseguire un upgrade. Basta smontare correttamente il file system Ext3 e montarlo in seguito come file system Ext2.

Affidabilità e prestazioni Altri journaling file system seguono l'approccio cosiddetto journaling metadata-only, cioè i vostri meta-dati rimangono in uno stato consistente, cosa che comunque non può essere garantita automaticamente per i dati del file system. Ext3 è in grado invece di assolvere entrambi i compiti, e persino il grado di consistenza si lascia impostare individualmente. Il più elevato grado di sicurezza (cioè integrità dei dati) si ottiene lanciando Ext3 nel modo `data=journal` che comunque può comportare un rallentamento del sistema, giacché vengono rilevati sia i meta-dati che i dati del journal. Un approccio relativamente recente consiste nell'utilizzo del modo `data=ordered` che provvede sia alla integrità dei dati che

dei meta-dati, ma che usa il journaling solo per i meta-dati. Il driver del file system raccoglie tutti i blocchi di dati appartenenti ad un aggiornamento dei meta-dati. Questi blocchi vengono scritti sul disco prima dell'aggiornamento dei meta-dati. In questo modo si ha una consistenza dei meta-dati e dei dati senza un calo di performance. Una terza possibilità consiste nel `data=writeback`. In questo caso i dati possono essere scritti nel file system principale dopo che i meta-dati sono stati consegnati al journal. Questa opzione è considerata da tanti la migliore sotto il punto di vista delle prestazioni. Comunque può accadere che ricompaiano nei file vecchi dati a seguito di un crash e ripristino, mentre è garantita l'integrità interna del file system. Se non avete cambiato impostazioni, Ext3 viene inizializzato nel modo `data=ordered`.

20.2.4 Convertire un file system Ext2 in uno Ext3

Tale processo si compone di due passaggi:

Creare il Journal Eseguite il log in come `root` ed eseguite `tune2fs -j`, con il quale create un journal Ext3 con i parametri di default. Per stabilire la dimensione del journal e su quale dispositivo debba risiedere, eseguite `tune2fs -J` con le opzioni desiderate riguardanti il journal `size=` e `device=`. Per maggiori informazioni sull programma tune2fs rimandiamo alla rispettiva pagina di manuale (tune2fs(8)).

Specificate il tipo di file system Type in /etc/fstab
Per assicurare che il file system Ext3 venga rilevato come tale, editate il file `/etc/fstab`: modificate il tipo di file system specificato per la partizione da `ext2` in `ext3`. Le modifiche vengono applicate al prossimo reboot.

Utilizzare Ext3 per la directory root Per avviare un file system root impostato come partizione Ext3, includete i moduli `ext3` e `jbd` in `initrd`. Per realizzare ciò, editate il file `/etc/sysconfig/kernel` per includere i due moduli sotto `INITRD_MODULES` ed eseguite il comando `mkinitrd`.

20.2.5 Reiser4

Dopo il rilascio del kernel 2.6, alla famiglia dei journaling file systems si è aggiunto un nuovo membro: Reiser4, il quale differisce completamente dal suo predecessore ReiserFS (versione 3.6). Reiser4, tramite dei plug-ins ottimizza le funzionalità del file system ed offre un concetto di sicurezza più sofistica.

Nuovo concetto di sicurezza In fase di sviluppo di Reiser4, gli sviluppatori hanno posto l'accento sull'implementazione di caratteristiche rilevanti da un punto di vista della sicurezza. Reiser4 offre quindi tutta una serie di plug-in preposti a incrementare la sicurezza. Nuovo in tal senso sono anche i file "items.". Attualmente, le regole di controllo di accesso vengono definite per ogni file. Se vi è un grande file con informazioni che interessano diversi utenti, gruppi o applicazioni, i permessi di accesso diventano poco precisi per non escludere nessuna delle parti interessate. Reiser4 vi permette di suddividere questi file (appunto in "items"). I permessi di accesso quindi possono essere impostati separatamente per ogni utente con dei benefici del security management. Un esempio ad-hoc è `/etc/passwd`. Finora, solo `root` poteva leggere ed editare il file, mentre tutti gli altri utenti hanno solo l'accesso in lettura. Tramite gli item di Reiser4, potete suddividere questo file in una serie di items (un item per utente) e dare il permesso agli utenti o applicazioni di modificare i propri dati, ma non di accedere ai dati di altri utenti. Questo approccio ha dei risvolti possitivi sia per la sicurezza che la flessibilità.

Scalabilità grazie ai plug-in In Reiser4 molte funzionalità del file system ed anche funzionalità esterne a cui ricorrono solitamente i file system sono stati implementati sotto forma di plug-in. Questi plug-in possono essere integrati in modo del tutto semplice nel sistema di base, quindi non si dovrà ricompilare il kernel o riformattare il disco rigido per intergrare delle nuove funzionalità al vostro file system.

Layout del file system ottimizzato grazie all'allocazione ritardata Alla stregua di XFS, Reiser4 supporta l'allocazione posposta. Si veda sezione 20.2.7 nella pagina successiva; questa funzionalità, se utilizzata per i metadata, contribuisce ad un miglior layout in generale.

20.2.6 JFS

JFS, il *Journaling File System*, è stato sviluppato da IBM per AIX. Nell'estate del 2000 esce la prima versione beta di JFS per Linux. La versione 1.0.0 è stata rilasciata nel 2001. JFS è tagliato per ambienti server con una elevata velocità di trasferimento dei dati (ingl. throughput), visto che in questo ambito quello che conta sono in prima linea le prestazioni. Essendo un file system a 64 bit, JFS supporta file voluminosi e partizioni (LFS ovvero Large File Support), caratteristica che lo qualifica ulteriormente per l'utilizzo in ambito server.

Se consideriamo più attentamente JFS scopriremo anche il motivo per cui questo file system si adatta bene ad un server Linux:

Journaling efficace JFS segue alla stregua di ReiserFS l'approccio "metadata only". Al posto di una verifica dettagliata vengono rilevati solo le modifiche apportate ai meta-dati dovute a recenti attività del file system. Questo permette di velocizzare considerevolmente il ripristino. Attività contemporanee che richiedono diversi registrazioni di protocollo possono essere raccolte in un cosiddetto commit di gruppo, laddove il calo dal punto di vista della prestazione del file system viene compensato dal processo di scrittura multipla.

Efficace amministrazione delle directory
JFS si orienta alla struttura della directory. Nel caso di piccole directory consente di salvare direttamente il contenuto della directory nel suo inode. Per directory più capienti utilizza alberi bilanciati (ingl. B^+trees) che semplificano notevolmente l'amministrazione delle directory.

Miglior sfruttamento della memoria attraverso l'allocazione dinamica degli inode
Sotto Ext2 dovete indicare a priori la densità degli inode (memoria occupata da informazioni di natura amministrativa). Questo impone un limite massimo di file o directory per il vostro file system. Con JFS invece la memoria inode viene assegnata dinamicamente e gli esuberi vengono subito messi nuovamente a disposizione del sistema.

20.2.7 XFS

Originariamente pensato come file system per il proprio sistema operativo IRIX, XFS è stato concepito dalla SGI già agli inizi degli anni '90 come journaling file system a 64 bit ad alte prestazioni per rispondere alle sempre crescenti richieste rivolte ad un file system moderno. XFS si adatta bene per file di una certa dimensione e dà prova di buona performance su hardware high-end. Comunque anche nel caso di XFS il tallone di Achille è rappresentato, come già per ReiserFS, dal fatto che XFS si concentra maggiormente sulla integrità dei meta-dati e meno sulla integrità dei dati.

Se osserviamo da vicino alcune funzionalità centrali di XFS vedremo il perché esso rappresenta una valida alternativa ad altri journaling file system in ambito della elaborazione dati high-end.

Alta scalabilità grazie agli "allocation groups"

Al momento della generazione di un file system XFS, il block device del file system viene suddiviso in otto o più settori lineari di ugual misura, detti "allocation groups" che chiameremo gruppi di allocazione. Ogni "gruppo di allocazione" gestisce gli inode e la memoria libera. I gruppi di allocazione sono in pratica dei "file system nei file system". Visto che i gruppi di allocazione sono in una certa misura autonomi, il kernel ha la possibilità di indirizzarne contemporaneamente più di uno. Ecco "il segreto" della alta scalabilità di XFS. Questa suddivisione in gruppi di allocazione è particolarmente indicata per sistemi multi-processore.

Alte prestazioni grazie ad una efficace amministrazione della memoria

La memoria libera e gli inode vengono gestiti da alberi B^+ all'interno dei gruppi di allocazione. Gli alberi B^+ contribuiscono in maniera determinante alla performance e alla scalabilità di XFS. Una caratteristica di XFS unica nel suo genere è la *delayed allocation*. XFS elabora l'assegnazione della memoria (ingl. allocation) bipartendo il processo. Una transazione "sospesa" viene memorizzata nella RAM e riservato il corrispondente spazio di memoria. XFS non stabilisce subito dove precisamente memorizzare i dati (cioè in quali blocchi del file system). Questa decisione viene rinviata il più possibile. Così file temporanei di breve durata non vengono scritti sul disco, visto che al momento di determinare la loro locazione sul disco sono già obsoleti. In tal modo XFS aumenta le prestazioni e riduce la frammentazione del file system. Dato però che una allocazione differita comporta un minor numero di accessi in scrittura rispetto ad altri file system, è probabile che la perdita di dati in seguito al verificarsi di un crollo durante il processo di scrittura risulterà essere maggiore.

Pre-allocazione per evitare la frammentazione del file system

Prima di scrivere i dati nel file system, XFS riserva lo spazio necessario per il file (ingl. preallocate). In questo modo si riduce notevolmente la frammentazione del file system, e si aumenta la performance, dato che il contenuto di un file non viene distribuito più lungo tutto il file system.

20.3 Ulteriori file system supportati

Tabella 20.1: *Tipi di file system sotto Linux*

`cramfs`	*Compressed ROM file system*: un file system compresso con accesso in lettura per ROM.
`hpfs`	*High Performance File System*: il file system standard di OS/2— supportato solo nella modalità di lettura.
`iso9660`	File system standard dei CD-Rom.
`minix`	File system per il mount di file system per dischetti.
`msdos`	*fat*, il file system utilizzato originariamente da DOS, oggi utilizzato da vari sistemi operativi.
`ncpfs`	File system per il mount di volumi Novell tramite la rete.
`nfs`	*Network File System*: in questo caso sussiste la possibilità di memorizzare i dati su un computer qualsiasi nella rete e di accedervi tramite la rete.
`smbfs`	*Server Message Block*: viene usato p.es. Windows per accedere a file tramite rete.
`sysv`	Viene utilizzato sotto SCO UNIX, Xenix e Coherent (sistemi commerciali UNIX per PC).
`ufs`	Viene utilizzato da BSD, SunOS e NeXTstep. Viene supportato solo nella modalità di lettura.
`umsdos`	*UNIX on MSDOS*: basato su un normale file system `fat`. Generando file speciali si ottengono funzionalità UNIX (permessi, link, file con nomi lunghi).
`vfat`	*Virtual FAT*: estensione del file system `fat` (supporta lunghi nomi di file).
`ntfs`	*Windows NT file system*, accesso in sola lettura.

20.4 Large File Support sotto Linux

Originariamente Linux supportava file fino a 2 GByte che bastava fino a che non si intendeva gestire delle voluminose banche dati con Linux. Visto il crescente significato della amministrazione di banche dati sotto Linux, o gestione dei dati audio e video etc, il kernel e la libreria GNU C sono stati modificati in modo da supportare file che superano il limite di 2 GByte. Vennero introdotte nuove interfacce che possono essere utilizzate dalle applicazioni. Oggi (quasi) tutti i principali file system supportano LFS che permette elaborazione di dati high-end. tabella 20.2 in questa pagina offre una rassegna dei limiti di file e file system Linux.

Tabella 20.2: *Dimensione massima dei file system(on-disk format)*

File system	Dim. file mass.	Dim. mass. file system
Ext2 o Ext3 (1 kB dim. di blocco)	2^{34} (16 GB)	2^{41} (2 TB)
Ext2 o Ext3 (2 kB dim. di blocco)	2^{38} (256 GB)	2^{43} (8 TB)
Ext2 o Ext3 (4 kB dim. di blocco)	2^{41} (2 TB)	2^{44} (16 TB)
Ext2 o Ext3 (8 kB dim. di blocco) (sistemi con pages di 8 kB (come 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 byte dim. di blocco)	2^{63} (8 EB)	2^{49} (512 TB)
JFS (4 kB dim. di blocco)	2^{63} (8 EB)	2^{52} (4 PB)
NFSv2 (lato client)	2^{31} (2 GB)	2^{63} (8 EB)
NFSv3 (lato client)	2^{63} (8 EB)	2^{63} (8 EB)

Importante

Limiti del kernel Linux

La tabella tabella 20.2 nella pagina precedente indica i limiti dell' on-disk format. La dimensione massima di un file e di un file system processata correttamente dal Kernel 2.6 sottosta alle seguenti restrizioni:

Dimensione del file: File e block device non possono superare i 2 TB (2^{41} byte) su sistemi a 32 bit.

Dimensione del file system: file system possono raggiungere una dimensione di 2^{73} byte. Questo limite non viene (ancora) sfruttato a fondo da nessun hardware attualmente reperibile.

Importante

20.5 Ulteriori fonti di informazioni

Ogni dei file system descritti ha un proprio sito web, dove è possibile reperire ulteriori informazioni grazie a mailing list, documentazione e FAQ.

- `http://e2fsprogs.sourceforge.net/ext2.html`
- `http://www.zipworld.com.au/~akpm/linux/ext3/`
- `http://www.namesys.com/`
- `http://oss.software.ibm.com/developerworks/opensource/jfs/`
- `oss.sgi.com/projects/xfs/`

Un tutorial completo dedicato ai file system Linux è rappresentato dall' *IBM developerWorks*; l'indirizzo è:`http://www-106.ibm.com/developerworks/library/l-fs.html`. Sotto *Linuxgazette*: `http://www.linuxgazette.com/issue55/florido.html` troverete un confronto dei vari journaling file system sotto Linux nell'articolo di Juan I. Santos Florido. Per un compendio di LFS sotto Linux visitate le pagine dedicate a LFS di Andreas Jaeger: `http://www.suse.de/~aj/linux_lfs.html`

Autenticazione con PAM

PAM (ingl. Pluggable Authentication Modules) viene utilizzato sotto Linux nel processo di autenticazione come layer che media tra l'utente e l'applicazione. I moduli PAM sono disponibili centralmente per tutto il sistema e possono essere invocati da ogni applicazione. Nel presente capitolo indicheremo come configurare il processo di autenticazione ed illustreremo il funzionamento del modulo.

A volte amministratori di sistema e sviluppatori desiderano limitare l'accesso a determinate aree di sistema o l'utilizzo di una determinata funzionalità di una determinata applicazione. Senza PAM ciò vorrebbe dire adattare continuamente le applicazioni ogni volta che si ricorre ad un nuovo meccanismo di autenticazione, come LDAP o SAMBA. Questo modo di procedere richiede tanto tempo ed è esposto ad errori. Se però il processo di autenticazione si svolge indipendentemente dall'applicazione e viene delegato a dei moduli centralizzati, si aggira questa difficoltà. Quando si vorrà applicare un nuovo schema di autenticazione, sarà sufficiente intervenire sul modulo PAM da cui l'applicazione riceverà le nuove indicazioni.

Per ogni programma che ricorre a PAM vi è un file di configurazione sotto `/etc/pam.d/<nomeprogramma>`. In questo file si determinano i moduli PAM da utilizzare ai fini dell'autenticazione degli utenti. La maggior parte dei file di configurazione generali dei moduli PAM sotto `/etc/security` determinano il comportamento dei moduli (esempi: `pam_env.conf`, `pam_pwcheck.conf`, `pam_unix2.conf`, `time.conf` etc.). Una applicazione che ricorre ad un modulo PAM invoca un determinato set di funzioni PAM, le quali dopo aver elaborato le informazioni nei diversi file di configurazione fanno pervenire il risultato alla applicazione richiedente.

21.1 Struttura di un file di configurazione PAM

Un rigo del file di configurazione PAM è composto al massimo di quattro colonne:

```
<Tipo_di_modulo> <Flag_di_controllo> <Percorso_del_modulo> <Opzioni>
```

Sono una serie di moduli PAM, detti anche stack (pila) di moduli, ad essere elaborati. I diversi moduli hanno funzioni diverse: un modulo si occupa della verifica della password, un altro verifica l'origine di un accesso ed un altro ancora si occupa delle impostazioni di sistema specifiche dell'utente. Esistono quattro tipi diversi di moduli PAM:

`auth` I moduli di questo tipo verificano l'autenticità dell'utente. La verifica si può basare sulla richiesta tradizionale della password, ma si può anche trattare di metodologie più avanzate come chip card o verifica di una caratteristica biometrica (impronta digitale, scansione dell'iride).

account I moduli di questo genere controllano se l'utente ha il permesso di utilizzare il servizio da lui richiesto. In tal modo gli utenti con un account non più valido, ovvero scaduto, non potranno più accedere ai servizi.

password Questo modulo viene usato per modificare il metodo di autenticazione, che il più delle volte è rappresentato da una password.

session I moduli di questo tipo servono all'amministrazione e configurazione della sessione utente. Questi moduli vengono inizializzati prima e dopo l'autenticazione, per protocollare i tentativi di login e per assegnare un ambiente all'utente (e-mail account, directory home, limiti riguardanti le risorse di sistema etc.).

La seconda colonna contiene i flag di controllo tramite i quali si chiamano in causa i moduli desiderati:

required Il modulo deve essere stato elaborato correttamente per proseguire nel processo di autenticazione. In caso contrario prima che l'utente riceva un avviso riguardante il tentativo di autenticazione fallito, vengono elaborati tutti gli altri moduli del tipo `required`

requisite Come per i moduli `required`, anche questi moduli devono essere elaborati in modo corretto ai fini dell'autenticazione. Se qualcosa non va per il verso giusto, l'utente viene avvisato immediatamente e fermato il processo di elaborazione dei moduli. Se tutto procede bene vengono elaborati gli altri moduli come con il flag `required`. Questo flag può essere impostato come semplice filtro per verificare se sono date determinate condizioni essenziali per una autenticazione corretta.

sufficient Se un modulo di questo tipo viene elaborato correttamente il programma che ha invocato i moduli di questo tipo riceve un relativo messaggio e non vengono elaborati gli altri moduli, sempre che con i moduli `required` è andato tutto per il verso giusto. Se un modulo `sufficient` non è stato elaborato correttamente, si prosegue semplicemente con l'elaborazione dei moduli successivi.

optional Non fa differenza se si ha una elaborazione coronata dal successo o meno; questa funzionalità viene utilizzata in prima linea con moduli che ad esempio indicano solo se un utente abbia ricevuto un e-mail o meno.

include Se è dato questo flag, il file specificato come argomento viene inserito qui.

Il percorso del modulo non viene indicato esplicitamente, se i moduli si trovano nella directory standard `/lib/security` (o rispettivamente sotto `/lib64/security` con piattaforme a 64 bit supportate da SUSE LINUX). Come quarta registrazione è possibile passare ancora una opzione al modulo, ad esempio `debug` (modo debug) o `nullok` (che consente password vuote).

21.2 La configurazione PAM di sshd

Dopo una introduzione teoretica ecco un esempio pratico riferito alla configurazione PAM di sshd:

Esempio 21.1: *Configurazione PAM per 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
```

La configurazione PAM tipica di una applicazione (in questo caso sshd) presenta quattro istruzioni riferite ai file di configurazione di quattro tipi di moduli: `common-auth`, `common-account`, `common-password`, e `common-session`. Questi quattro file contengono la configurazione di default per ogni tipo di modulo. Includendoli, invece di invocare singolarmente ogni modulo per ogni applicazione PAM, si ha automaticamente una configurazione PAM aggiornata qualora l'amministratore di sistema modificasse i valori di default. In passato si dovevano adattare manualmente tutti i file di configurazione per tutte le applicazioni quando si apportavano delle modifiche a PAM o quando si installavano delle nuove applicazioni. Ora la configurazione PAM avviene tramite file di configurazione centrali, e quindi in caso di modifiche, esse vengono ereditate dalla rispettiva configurazione PAM del servizio in questione.

Il primo file include (`common-auth`) invoca due moduli del tipo `auth`: `pam_env` e `pam_unix2`. Si veda l'esempio 21.2 a fronte.

Esempio 21.2: *Configurazione di default per la sezione* `auth`

```
auth    required        pam_env.so
auth    required        pam_unix2.so
```

`pam_env` legge il file `/etc/security/pam_env.conf` ed imposta le variabili di ambiente stabilite in questo file. Qui ad esempio potete impostare il valore corretto per la variabile `DISPLAY`, visto che `pam_env` contiene delle informazioni riguardanti la postazione dalla quale un utente tenta di eseguire il login. `pam_unix2`, esegue una verifica del login dell'utente e della password in base a `/etc/passwd` e `/etc/shadow`.

Dopo che i moduli specificati in `common-auth` sono stati invocati correttamente, un terzo modulo chiamato `pam_nologin` verifica l'esistenza del file `/etc/nologin`. In caso affermativo, nessun altro utente all'infuori di `root` può eseguire il log in. La pila dei moduli di `auth` viene elaborata prima che sshd riceva dell'informazioni sulla riuscita o meno del tentativo di log in. Dato che tutti moduli della pila hanno il flag di controllo `required`, essi dovranno essere tutti elaborati correttamente prima che sshd riceva una comunicazione riguardante l'esito positivo o meno. Se l'elaborazione di uno dei moduli non porta all' esito positivo, si continuerà con l'elaborazione dell'intera pila di moduli prima che venga comunicato a sshd che l'esito è stato negativo.

Non appena tutti i moduli del tipo `auth` siano stati elaborati correttamente, viene elaborata un'altra istruzione include, in questo case quella nell'esempio 21.3 in questa pagina. `common-account` contiene solo un modulo: `pam_unix2`. Se `pam_unix2` comunica che l'utente esistet, sshd riceve la rispettiva comunicazione e si prosegue con l'elaborazione della prossima pila di moduli (`password`) come mostrato nell'esempio 21.4 in questa pagina.

Esempio 21.3: *Configurazione di default per la sezione* `account`

```
account required        pam_unix2.so
```

Esempio 21.4: *Configurazione di default per la sezione* `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
```

Nuovamente la configurazione di sshd involve solo una istruzione include riferita alla configurazione di default per moduli `password`, residenti in `common-password`. Questi moduli devono essere elaborati correttamente (flag di controllo: `required`), se l'applicazione richiede una modifica del cosiddetto token di autenticazione. Quando si intende modificare una password o un altro token di autenticazione viene eseguita una verifica della sicurezza, cosa che viene realizzata dal modulo `pam_pwcheck`. Il modulo `pam_unix2` assume le vecchie e nuove password da `pam_pwcheck` in modo che l'utente non dovrà autenticarsi nuovamente. Inoltre in tal modo si evita che si aggirino le verifiche di `pam_pwcheck`. I moduli del tipo `password` vanno invocati se i moduli preposti a `account` o `auth` segnalano una password scaduta.

Esempio 21.5: *Configurazione di default per la sezione* `session`

```
session required        pam_limits.so
session required        pam_unix2.so
```

Infine vengono inizializzati i moduli di tipo `session` riuniti nel file `common-session` per configurare la sessione dell'utente in base alle impostazioni previste. Il modulo `pam_unix2` viene invocato nuovamente ma a causa dell'opzione `none` specificata nel rispettivo file di configurazione del modulo, ossia `pam_unix2.conf`, questa chiamata non produce alcun effetto. Il modulo `pam_limits` legge il file `/etc/security/limits.conf` in cui possono essere stabiliti dei limiti riguardanti l'utilizzo delle risorse di sistema. Quando l'utente esegue il logout vengono invocati nuovamente i moduli `session`.

21.3 Configurazione del modulo PAM

Tramite i relativi file di configurazione potete intervenire sulla configurazione dei moduli PAM. Questi file si trovano sotto `/etc/security`. Questa sezione tratta brevemente i file relativi all'esempio sshd, ovvero `pam_unix2.conf`, `pam_env.conf`, `pam_pwcheck.conf` e `limits.conf`.

21.3.1 pam_unix2.conf

Per l'autenticazione basata su password tradizionale si ricorre al modulo PAM `pam_unix2` che recupera i dati richiesti da `/etc/passwd`, `/etc/shadow`,

da cosiddette mappe NIS, tabelle NIS+ o da una banca dati LDAP. Sussiste la possibilità di influire sul comportamento del modulo configurando le opzioni PAM per l'applicazione in questione oppure in modo globale intervenendo su `/etc/security/pam_unix2.conf`. Un file di configurazione di base per il modulo viene riportato nell'esempio 21.6 in questa pagina.

Esempio 21.6: *pam_unix2.conf*

```
auth:           nullok
account:
password:       nullok
session:        none
```

L'opzione `nullok` per i tipi di modulo `auth` e `password` indica che sono ammesse password vuote per questo tipo di account. L'utente ha il permesso di cambiare password. Tramite l'opzione `none` per il tipo di modulo `session` si stabilisce che per questo tipo di modulo non viene protocollato alcun messaggio (impostazione di default). Per ulteriori opzioni di configurazione rimandiamo ai commenti nel file o alla pagina di manuale di pam_unix2 (8).

21.3.2 pam_env.conf

Questo file viene utilizzato per assegnare all'utente, dopo aver invocato il modulo `pam_env`, un ambiente standardizzato. La sintassi per settare le variabili di ambiente è:

```
VARIABILE  [DEFAULT=[valore]]  [OVERRIDE=[valore]]
```

`VARIABILE` Nome della variabile di ambiente da settare.

`[DEFAULT=[valore]]` Valore di default che l'amministratore intende impostare.

`[OVERRIDE=[valore]]` Valori impostabili da `pam_env` che sovrascrivono il valore di default.

Un esempio diffuso in cui `pam_env` sovrascrive dei valori di default interessa la variabile `DISPLAY` che viene modificata ad ogni login da remoto: si veda l'esempio 21.7 nella pagina seguente.

Esempio 21.7: *pam_env.conf*

```
REMOTEHOST      DEFAULT=localhost OVERRIDE=@{PAM_RHOST}
DISPLAY         DEFAULT=${REMOTEHOST}:0.0 OVERRIDE=${DISPLAY}
```

Il primo rigo imposta il valore della variabile `REMOTEHOST` su `localhost`, se `pam_env` non riesce a rilevare un altro valore. La variabile `DISPLAY` ricorre al valore di `REMOTEHOST`. Per maggiori informazioni rimandiamo ai commenti del file `/etc/security/pam_env.conf`.

21.3.3 pam_pwcheck.conf

Da questo file il modulo `pam_pwcheck` recupera le opzioni per tutti i moduli del tipo `password`. Le impostazioni qui salvate vengono lette prima di quelle delle impostazioni PAM dell'applicazione. Se per l'applicazione non è stata eseguita alcuna impostazione individuale, verrà applicata quella globale. L'esempio 21.8 in questa pagina indica a `pam_pwcheck` di consentire password vuote e la modifica delle password. Per le altre opzioni disponibili per il modulo rimandiamo al file `/etc/security/pam_pwcheck.conf`.

Esempio 21.8: *pam_pwcheck.conf*

```
password:    nullok
```

21.3.4 limits.conf

Le restrizioni che interessano l'utilizzo delle risorse del sistema possono essere impostate a livello utente o a livello di gruppo nel file `limits.conf` che viene letto dal modulo `pam_limits`. In teoria sussiste la possibilità di impostare dei limiti rigidi (impossibili da sforare) e dei limiti flessibili (con possibilità di sforamento temporaneo) per le risorse di sistema. La sintassi e le opzioni consentite sono reperibili nel file stesso.

21.4 Ulteriori informazioni

Sul vostro sistema installato trovate nella directory `/usr/share/doc/packages/pam` la seguente documentazione:

README La directory principale include alcuni README di natura generale. Nella sottodirectory `modules` vi sono i README per i moduli PAM disponibili.

The Linux-PAM System Administrators' Guide
Tutto quello che vale la pena di sapere su PAM come amministratore di sistema. Qui vengono trattate tematiche che spaziano dalla sintassi di un file di configurazione PAM fino ad arrivare agli aspetti riguardanti la sicurezza di PAM. Le informazioni sono disponibili nei formati PDF, HTML o testo semplice.

The Linux-PAM Module Writers' Manual
Qui sono raccolte le informazioni necessarie allo sviluppatore per scrivere moduli PAM conformi agli standard. Queste informazioni sono disponibili nei formati PDF, HTML o testo semplice.

The Linux-PAM Application Developers' Guide
Questo documento contiene tutto quello uno sviluppatore di applicativi deve sapere se intende utilizzare librerie PAM. Queste informazioni sono disponibili nei formati PDF, HTML o testo semplice.

Per un'introduzione di base alla tematica PAM, redatta da Thorsten Kukuk, sviluppatore di una serie di moduli PAM per SUSE LINUX, rimandiamo a `http://www.suse.de/~kukuk/pam/`.

Parte III

Servizi

Fondamenti del collegamento in rete

Linux, che è nato grazie all'Internet, offre tutti gli strumenti di rete necessari per essere integrato in diverse strutture di rete. In questo capitolo, vi presentiamo il protocollo TCP/IP usato solitamente da Linux, con tutti i suoi servizi e le sue proprietà. Vi mostreremo come realizzare con l'aiuto di YaST l'accesso alla rete utilizzando una scheda di rete, modem o altro dispositivo. Potete anche eseguire la configurazione manualmente. Parleremo dei file centrali di configurazione e verranno illustrati alcuni dei tool principali.

Linux ed altri sistemi operativi Unix usano il cosiddetto protocollo TCP/IP: in fondo si tratta di un gruppo di protocolli che offre svariati servizi. TCP/IP deriva da uno sviluppo di applicazioni in ambito militare e, nella forma usata oggi, è stato definito circa nel 1981 in un cosiddetto RFC Request for comments; i protocolli elencati in tabella 22.1 in questa pagina permettono lo scambio di dati tra due macchine tramite TCP/IP. TCP/IP è il protocollo che connette la rete globale nota anche sotto il nome di "Internet."

RFC *Request for Comments* sono dei documenti che descrivono i diversi protocolli Internet ed il procedimento da seguire per l'implementazione del sistema operativo e delle applicazioni. Potete consultare direttamente questi documenti RFC tramite il web: l'URL è: `http://www.ietf.org/`.

Tabella 22.1: *Diversi protocolli del gruppo di protocolli TCP/IP*

Protocollo	**Descrizione**
TCP	Transmission control protocol: protocollo orientato alla connessione. Dal punto di vista dell'applicazione, i dati da trasmettere vengono inviati sotto forma di flusso di dati e convertiti dal sistema operativo stesso nel formato adatto alla trasmissione. I dati arrivano all'applicazione-meta che si trova sul computer-meta nella sequenza in cui sono stati spediti. TCP assicura che non vadano persi dei dati durante la trasmissione, e che non vengano mescolati. TCP viene usato dove è saliente la sequenza dei dati.
UDP	User Datagram protocol: un protocollo non orientato alla connessione: i dati vengono spediti in pacchetti, ed i pacchetti di dati vengono generati dall'applicazione. Non è garantito che i dati arrivano nella sequenza esatta al destinatario, e non è escluso che si possa verificare la perdita di singoli pacchetti. UDP è adatto per applicazioni orientati al set di dati, e ha tempi di latenza inferiori al TCP.

ICMP	Internet control message protocol: fondamentalmente, questo non è un protocollo pensato per gli utenti, ma uno speciale protocollo di controllo che trasmette comunicazioni di errore, ed è in grado di controllare il comportamento dei sistemi coinvolti nella trasmissione di dati tramite TCP/IP. Inoltre, con ICMP, viene messo a disposizione anche uno speciale "modo echo" che può venire esaminato con il programma ping.
IGMP	Internet group management protocol: questo protocollo regola il comportamento dei sistemi che usano il multicast IP. Purtroppo, in questa sede non possiamo entrare nei dettagli del multicasting IP.

Come mostrato nella figura 22.1 in questa pagina nello scambio di dati son coinvolti una serie di strati. Tramite IP (Internet protocol) si ha una trasmissione di dati non garantita. Il TCP (Transmission control protocol) poggia in un certo senso sul sottostante IP, volto a garantire una trasmissione sicura dei dati. IP a sua volta poggia sul protocollo sottostante che dipende dall'hardware, p.es. Ethernet.

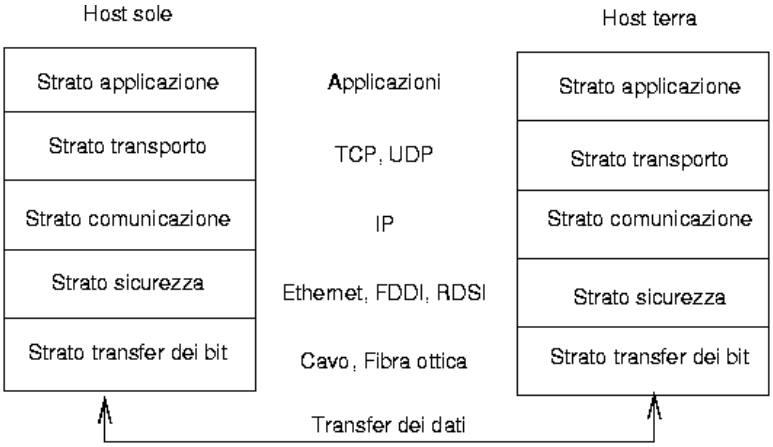

Figura 22.1: *Modello a strati semplificato per TCP/IP*

Nella figura vengono menzionati degli esempi per il rispettivo strato. Come vedete, gli strati sono disposti secondo dei "livelli di astrazione"; lo strato inferiore è molto vicino all'hardware. Lo strato superiore invece, astrae quasi completamente dall'hardware sottostante. Ogni strato ha una funzione speciale che si deduce quasi già dal nome. Ad esempio, la rete usata (p.es. Ethernet) viene rapprensentata dallo strato di trasmissione dei bit e dallo strato di sicurezza.

Quasi tutti i protocolli hardware lavorano a pacchetti. I dati da trasmettere vengono riuniti in piccoli "pacchetti", e non possono venire spediti in una volta sola. Per questo motivo, TCP/IP lavora con piccoli pacchetti di dati. La dimensione massima di un pacchetto TCP/IP è di appena 64 Kbyte. Normalmente, i pacchetti sono molto più piccoli, poiché l'hardware della rete è un fattore limitante: ad esempio, le dimensioni di un pacchetto di dati su Ethernet sono limitate a 1500 byte. Il dimensionamento del pacchetto TCP/IP viene limitato di conseguenza (se i dati vengono trasmessi tramite Ethernet). Nel caso si vogliono trasmettere più dati, il sistema operativo deve inviare più pacchetti di dati.

Affinché ogni strato possa adempiere alla sua funzione, si devono aggiungere al pacchetto determinate informazioni dallo strato corrispondente. Ciò avviene nell'*header*, l'intestazione del pacchetto di dati. Ogni strato aggiunge, all'inizio del pacchetto in via di formazione, un piccolo blocco di dati, la cosiddetta "testata del protocollo" (ingl. protocol header). Un qualsiasi pacchetto di dati TCP/IP trasmesso tramite un cavo Ethernet è strutturato come rappresentato nella figura 22.2 a fronte. La somma di controllo si trova alla fine del pacchetto e non all'inizio. Ciò semplifica le cose per l'hardware di rete.

Se dunque, un'applicazione invia dei dati tramite una rete, questi attraversano i singoli strati che sono tutti implementati nel kernel di Linux (ad eccezione dello strato 1: la scheda di rete). Ogni strato deve trattare i dati in modo da poterli passare di volta in volta allo strato inferiore. L'ultimo strato infine, ha il compito di spedire i dati. Al ricevimento dei dati, le cose si svolgono all' incontrario; vengono eliminate le testate dei protocolli di ogni strato e rimangono i dati utente (proprio come quando si sbuccia una cipolla). Alla fine, lo strato 4 deve mettere a disposizione i dati per le applicazioni sul computer-meta. Durante questo processo uno strato comunica sempre solo con quello direttamente superiore o inferiore. Per un'applicazione, non fa perciò differenza se i dati vengano trasmessi tramite una rete FDDI di 100 MBit/s o tramite un modem di 56 kbit/s: d'altra parte, per la trasmissione dei dati non importa quali dati vengano trasmessi, purché siano impacchettati nel modo giusto.

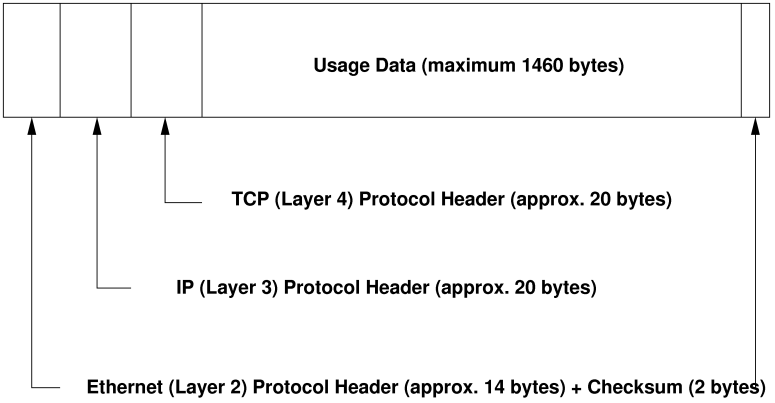

Figura 22.2: *Pacchetto TCP/IP nell'Ethernet*

22.1 Indirizzi IP e routing

Nei seguenti paragrafi presentiamo una descrizione di reti IPv4. Per delle informazioni riguardanti IPv6 consultate la sezione 22.2 a pagina 405.

22.1.1 Indirizzi IP

Ogni computer su Internet ha un indirizzo di 32 bit univoco. Normalmente, questi 32 bit o 4 byte vengono scritti come mostrato nella seconda riga dell'esempio 22.1 in questa pagina:

Esempio 22.1: *Sintassi di un indirizzo IP*

```
Indirizzo IP (binario):   11000000 10101000 00000000 00010100
Indirizzo IP (decimale):      192.     168.       0.      20
```

I quattro byte vengono scritti l'uno accanto all'altro nel modo decimale, e separati da un punto. L'indirizzo IP viene assegnato ad un computer o ad un'interfaccia di rete, e non può quindi venire assegnato nuovamente. Ci sono eccezioni alla regola che comunque non ci interessano nelle seguenti considerazioni.

Anche la scheda Ethernet possiede un proprio indirizzo: si tratta del cosiddetto indirizzo *MAC* (ingl. Media access control), un indirizzo di 48 bit, unico in tutto il mondo e memorizzato dal produttore della scheda di rete nell'hardware. Lo svantaggio di questo indirizzo fisso di fabbrica consiste nel fatto che gli indirizzi—*MAC* non formano un sistema gerarchico, vengono piuttosto assegnati in modo più o meno casuale, e quindi non sono adatti all'indirizzamento di host remoti. L'indirizzo *MAC* svolge però un ruolo di primo piano nella comunicazione tra gli host in una rete locale (e rappresenta la componente principale della testata del protocollo dello strato 2).

Ed ora torniamo agli indirizzi IP: i punti ci indicano già che gli indirizzi IP formano un sistema gerarchico. Fino alla metà degli anni 90, questi indirizzi erano suddivisi in classi: questo sistema si dimostrò però troppo inflessibile, e questa suddivisione venne subito abbandonata. Ora si usa il "routing libero" (CIDR classless inter domain routing).

22.1.2 Maschere di rete e routing

Poiché, in un primo tempo, il computer con l'indirizzo IP 192.168.0.1 non può sapere dove trovare il computer con l'indirizzo IP 192.168.0.20, si escogitò la maschera rete. Detto in parole semplici, la maschera di rete di un host con l'indirizzo IP definisce cosa si trova "dentro" e cosa si trova "fuori" la rete locale. I sistemi che si trovano "dentro" (in gergo "nella stessa sottorete") possono essere indirizzati direttamente; quelli invece che si trovano "fuori" ("che quindi non sono nella stessa sottorete") della rete locale, devono essere indirizzati tramite un gateway o router. Dato che ogni interfaccia di rete può avere un proprio indirizzo IP, avrete intuito che la faccenda può diventare davvero complessa.

Ecco cosa avviene nel computer, prima che possa venire "instradato" un pacchetto: l'indirizzo meta viene collegato bit dopo bit con la maschera rete tramite l'operatore logico AND; successivamente anche l'indirizzo del mittente viene collegato bit dopo bit con la maschera di rete tramite l'operatore logico AND. Se non vi sono delle discrepanze, il sistema meta si trova nella stessa sottorete, in caso contrario esso dovrà essere indirizzato tramite un gateway. Ciò significa che più bit "1" si trovano nella maschera di rete, meno sistemi possono venire indirizzati direttamente, e che dunque si dovrà passare per un gateway. A scopo esplicativo abbiamo elencato alcuni esempi nella esempio 22.2 nella pagina successiva.

Esempio 22.2: *Abbinare indirizzo IP con la maschera di rete*

```
Indirizzo IP (192.168.0.20):       11000000 10101000 00000000 00010100
Maschera di rete  (255.255.255.0): 11111111 11111111 11111111 00000000
_____________________________________________________________________
Risultato (binario):               11000000 10101000 00000000 00000000
Risultato (decimale):                   192.     168.       0.       0

Indirizzo IP (213.95.15.200):      11010101 10111111 00001111 11001000
Maschera di rete (255.255.255.0):  11111111 11111111 11111111 00000000
---------------------------------------------------------------------
Risultato (binario):               11010101 10111111 00001111 00000000
Risultato (decimale):                   213.      95.      15.       0
```

Anche la maschera di rete (come già gli indirizzi IP) viene scritta in numeri decimali divisi da punti, e poiché la maschera di rete ha un valore di 32 bit, si hanno 4 valori numerici l'uno accanto l'altro. L'utente deve stabilire quale host debba fungere da gateway o quali aree di indirizzi debbano essere raggiungibili tramite quale interfaccia di rete.

Per esempio, di solito tutti i sistemi collegati allo stesso cavo Ethernet, si trovano *nella stessa sottorete*, e sono indirizzabili in modo diretto. Anche se l'Ethernet è suddiviso per via di cosiddetti switch o bridge, questi sistemi continuano ad essere indirizzabili in modo diretto.

Ethernet, anche se vantaggioso da un punto di vista del costo, non è indicato per coprire distanze lunghe, quindi dovrete inoltrare i pacchetti IP ricorrendo ad un altro tipo di hardware (p.es. FDDI o ISDN): a tal fine si usano dei dispositivi chiamati router o gateway. Naturalmente, anche un computer Linux può fungere da router o gateway; basta impostare l'opzione relativa che è `ip_forwarding`.

Se avete configurato un gateway, il pacchetto IP viene inviato al gateway appropriato che a sua volta cerca di inoltrarlo (sempre sulla base dello stesso schema). Ciò viene ripetuto su una serie di computer, finchè il pacchetto non raggiunge la sua destinazione o scade il TTL time to live del pacchetto.

Tabella 22.2: *Indirizzi speciali*

Tipo di indirizzo	Descrizione
Indirizzo base della rete	Si tratta dell'indirizzo della maschera di rete abbinato ad un indirizzo qualsiasi preso dalla rete: cioé ciò che è raffigurato nell'esempio 22.2 nella pagina precedente sotto `Risultato`. Questo indirizzo non può venire assegnato ad alcun computer.
L'indirizzo broadcast	Broadcast vuol dire: "contatta tutti i computer in questa sottorete". Per crearlo, si inverte in modo binario l'indirizzo della maschera di rete e lo si abbina all'indirizzo di base della rete con l'operatore logico OR. Dal suddetto esempio risulta quindi 192.168.0.255. Chiaramente, neanche questo indirizzo può essere attribuito ad alcun computer.
Il local host	L'indirizzo `127.0.0.1` è attribuito permanentemente su ogni computer al cosiddetto "dispositivo di loopback". Con questo indirizzo si può creare un collegamento con la vostra macchina.

Poiché, però, in tutto il mondo, gli indirizzi IP devono essere biunivoci, non si possono inventare indirizzi qualsiasi. Per poter però creare ugualmente una rete sulla base dell'IP, esistono tre aree di indirizzi da poter usare senza restrizione alcuna: con esse però non sarà possibile (senza usare qualche trucco) creare un collegamento verso l'esterno ovvero raggiungere l'Internet; su Internet, infatti, questi indirizzi non vengono inoltrati. Si tratta delle aree di indirizzi definite nell' RFC 1597 ed elencati nella tabella 22.3 in questa pagina:

Tabella 22.3: *Aree indirizzi IP privati*

Rete/ maschera di rete	Area
`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 – l'Internet di prossima generazione

Come conseguenza del boom del World Wide Web e con esso il numero dei sistemi che comunicano utilizzando il linguaggio TCP/IP, è cresciuto in modo esponenziale; e da quando, nel 1990, Tim Berners-Lee del CERN `http://public.web.cern.ch/` ha inventato il www, il numero degli host presenti su Internet è passato da poche migliaia a ca. 100 milioni.

Come detto, un indirizzo IP è formato "solo" da 32 bit. Alcuni indirizzi IP rimangono inutilizzati per motivi che illustreremo di seguito. Inoltre, l'Internet è suddiviso in sottoreti, cioè in reti parziali che si compongono di un valore alla potenza di due meno due indirizzi IP. Per esempio, una sottorete consiste di 2, 6, 14, 30, etc. indirizzi IP. Se, per esempio, volete collegare 128 computer ad Internet, avete bisogno di una sottorete della con 256 indirizzi IP, dei quali potete utilizzare effettivamente solo 254. Come avete visto sopra, in una sottorete vengono a mancare 2 degli indirizzi IP, e cioè l'indirizzo broadcast e l'indirizzo di base della rete.

Per evitare l'esaurirsi degli indirizzi disponibili sotto IPv4 si ricorre a meccanismi del tipo DHCP o NAT Network Address Translation che, assieme alla suddivisione degli spazi di indirizzi in pubblici e privati, contribuiscono a migliorare la situazione su questo fronte. Lo svantaggio di questi meccanismi è che non sono facili da configurare e amministrare. Per la configurazione corretta di un host in una rete IPv4 sono necessarie una serie di dati come il proprio indirizzo IP, la maschera della sottorete, l'indirizzo gateway ed eventualmente un server dei nomi. Tutte queste informazioni le dovete "conoscere" visto che non vi è alcun modo di dedurrle.

Con IPv6 numero insufficente di indirizzi e configurazione complicata appartengono al passato. Nelle seguenti sezioni illustreremo le novità ed i vantaggi di IPv6 rispetto alla versione di protocollo precedente.

22.2.1 Vantaggi di IPv6

Il vantaggio più lampante del nuovo protocollo è l'enorme estensione dello spazio di indirizzamento. Un indirizzo IPv6 ha 128 bit rispetto ai 32 bit di IPv4. In tal modo il numero degli indirizzi IP disponibili raggiunge svariati migliaia di miliardi!

Gli indirizzi IPv6 non si distinguono dai loro predecessori solo per la loro lunghezza, ma anche per la loro struttura interna che consente di codificare delle

informazioni inerenti al sistema e alla rete. Per maggiori informazioni, leggete la sezione 22.2.2 a fronte.

Ulteriori vantaggi del nuovo protocollo in rassegna:

Configurazione automatica IPv6 applica il principio del "plug-and-play" nell' ambito della rete. Un sistema appena installato si lascia integrare nella rete (locale) senza dover intervenire sulla configurazione. Durante la configurazione automatica il terminale deduce il proprio indirizzo dalle informazioni che gli giungono dal protcollo "Neighbor Discovery" (ND) dai router adiacenti. Questo processo non richiede alcun intervento da parte dell'amministratore, e rispetto al DHCP, utilizzato per allocare gli indirizzi sotto IPv4, vi è inoltre il vantaggio di non dovere più amministrare un server centrale con gli indirizzi disponibili.

Mobilità IPv6 consente di allocare contemporaneamente più indirizzi ad una interfaccia di rete. In tal modo, realizzate con il minimo sforzo l'accesso a diverse reti. Questa funzionalità si lascia paragonare a quella del "roaming" che conoscete dal mondo dei telefonini: se vi trovate all'estero con il vostro telefonino, esso entra automaticamente nella rete estera. Indipendentemente dalla vostra locazione, siete raggiungibili sotto il vostro numero di cellulare consueto, e potrete continuare a telefonare normalmente anche all'estero come se vi trovaste nella rete del vostro fornitore di servizio.

Comuncazione sicura Mentre sotto IPv4 per realizzare una comunicazione sicura bisognava ricorrere ad una funzionalità aggiuntiva, IPv6 contiene già IPSec che garantisce una comunicazione sicura tra due sistemi collegati via Internet tramite un tunnel.

Compatibilità con IPv4 É impensabile che su Internet si passi di colpo da IPv4 a IPv6. Ecco spiegato il perché della necessità di una coesistenza delle due versioni sia su Internet che anche su di un sistema. Su Internet la coesistenza dei due protocolli viene resa possibile attraverso l'utilizzo di indirizzi compatibili (indirizzi IPv4 si lasciano facilmente convertire in indirizzi IPv6) e l'utilizzo di diversi tunnel (si veda la sezione 22.2.3 a pagina 411). Grazie al "dual-stack-IP" entrambi i protocolli vengono supportati anche da singoli sistemi. Ognuno dei due protocolli utilizza un proprio stack di rete, per evitare delle interferrenze tra le due versioni del protocollo.

Multicasting – servizi su misura Mentre sotto IPv4 alcuni servizi di sistema (p.es. SMB) devono inviare i propri pacchetti dati via broadcast agli host della rete locale, sotto IPv6 potete procedere in modo più differenziato.

Tramite un *multicasting* potete indirizzare contemporaneamente un gruppo di host, dunque non dovete necessariamente indirizzare tutti come è il caso per il (*broadcast*), oppure solo uno come nel caso del (*unicast*). L'applicazione determina quale gruppo sarà quello ad essere indirizzato. Vi sono anche dei gruppi multicast ben definiti, come ad esempio *tutti i server dei nomi* (ingl. all nameservers multicast group), oppure *tutti i router* (ingl. all routers multicast group).

22.2.2 Il sistema degli indirizzi IPv6

Come già accennato, il protocollo IP finora utilizzato comporta due vistosi svantaggi: da una parte si esauriscono man mano gli indirizzi IP disponibili e dall'altra l'amministrazione della rete e delle tabelle di routing diventa sempre più laboriosa. Il primo problema viene risolto con IPv6 attraverso un ampliamento dello spazio di indirizzamento a 128 bit; il secondo attraverso una struttura gerarchica degli indirizzi, raffinati meccanismi preposti all'allocazione dell'indirizzo di rete e la possibilità del *multi-homing* (diversi indirizzi per ogni interfaccia di rete con accesso a reti diverse).

Per quel che riguarda IPv6 si distinguono i seguenti tre tipi di indirizzi:

unicast Gli indirizzi di questo tipo vengono assegnati ad una determinata interfaccia di rete. I pacchetti con un indirizzo di tipo unicast vengono consegnati ad un solo destinatario. Attraverso indirizzi unicast si indirizzano singoli host all'interno della rete locale o su Internet.

multicast Gli indirizzi di questo tipo identificano un gruppo di interfacce. I pacchetti con un indirizzo di questo tipo vengono inviati a tutti i destinatari appartenenti ad un determinato gruppo. Gli indirizzi multicast vengono utilizzati in prima linea da determinati servizi di rete per indirizzare in modo mirato un determinato gruppo di host.

anycast Anche gli indirizzi di questo tipo fanno riferimento ad un gruppo di interfacce. I pacchetti con un indirizzo di questo tipo vengono consegnati al componente del gruppo che in base al protocollo di routing si trova il più vicino al mittente. Gli indirizzi anycast vengono utilizzati per consentire al terminale di rilevare il server richiesto all'interno della propria rete. Tutti i server di un determinato tipo hanno assegnato lo stesso indirizzo anycast. Quando un terminale richiede un servizio, risponderà il server che secondo il protocollo di routing è quello meno distante dall'host. Se questo server

per un motivo qualsiasi non è in esecuzione, si ricorrerà automaticamente al prossimo server in termini di vicinanza ....

L'indirizzo IPv6 è composto da otto blocchi di 16 bit ciascuno, separati dal segno `:` (due punti) disposti nel modo esadecimale. Gli zero byte all'inizio di un gruppo possono essere ommessi, ma non quelli in mezzo od alla fine di un gruppo. Si possono saltare più di quattro zero byte susseguenti in modo diretto tramite un carattere di ommissione `::`. Comunque, un indirizzo può contenere solamente un carattere di ommissione. In inglese si usa il termine "collapsing" per descrivere questo procedimento. L'output dell'esempio 22.3 in questa pagina vi mostra questo procedimento con tre modi di rappresentare lo stesso indirizzo.

Esempio 22.3: *Esempio di un indirizzo IPv6*

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                            : 10 : 1000 : 1a4
```

Ogni sezione dell'indirizzo IPv6 ha un significato ben preciso. I primi byte compongono il prefisso, ed indicano il tipo di indirizzo. La parte centrale indirizza una rete o non è rilevante, e la parte finale dell'indirizzo è la sezione host. In IPv6 le maschere di rete vengono definite tramite la lunghezza del prefisso, e vengono aggiunte all'indirizzo tramite un `/`. Nell' indirizzo dell'output dell'esempio 22.4 in questa pagina gli ultimi 64 bit indicano la sezione dell'host, ed i primi 64 bit la sezione della rete dell' indirizzo. Detto diversamente `64` indica che la maschera di rete viene riempita a partire da sinistra con una serie di 1 bit. Dunque nella maschera di rete abbiamo 64 1 bit. Come anche per IPv4, attraverso un collegamento AND della maschera di rete ed indirizzo IP viene stabilito se un host si trova all'interno o all' infuori di una determinata sottorete.

Esempio 22.4: *Indirizzo IPv6 con prefisso*

```
fe80::10:1000:1a4/64
```

IPv6 ha diversi prefissi che hanno un significato ben preciso (si veda la tabella 22.4 a fronte).

Tabella 22.4: *diversi prefissi IPv6*

Prefisso (esadec.)	Uso
`00`	Indirizzo IPv4 ed IPv4 tramite indirizzi di compatibilità IPv6: si tratta di un indirizzo compatibile con IPv4. Un router adatto trasforma il pacchetto IPv6 in IPv4. Anche altri indirizzi speciali (p.es. dispositivi loopback) sono muniti di questo prefisso.
Prima cifra`2` o `3`	(ingl. Aggregatable Global Unicast Adress). Anche sotto IPv6 vi possono essere delle sottoreti. Al momento vi sono a riguardo le seguenti aree di indirizzo: `2001::/16` (*production quality address space*) e `2002::/16` (*6to4 address space*).
`fe80::/10`	Indirizzi link-local con questo prefisso non vengono instradati (routed), e perciò possono essere indirizzati solo all'interno della stessa sottorete.
`fec0::/10`	(ingl. site-local) Questi indirizzi possono venire instradati (routed), ma solo all' interno di un sito. Così, questi indirizzi sono paragonabili alle reti "private" (p.es. `10.x.x.x`).
`ff`	Indirizzi IPv6 multicast che iniziano con `ff` sono indirizzi multicast.

Gli indirizzi unicast sono composti da tre parti:

Public Topology La prima parte, che include tra l'altro uno dei prefissi menzionati sopra, serve per il routing ovvero l'instradamento del pacchetto su Internet. Qui sono codificate delle informazioni sul provider o istituzione tramite cui si realizza l'accesso alla rete.

Site Topology La seconda parte contiene delle informazioni di routing riguardanti la sottorete meta del pacchetto.

Interface ID La terza parte identifica l'interfaccia a cui viene inviato il pacchetto. Questo consente di utilizzare l'indirizzo MAC come componente dell'indirizzo. Visto che nel mondo non vi sono due indirizzi MAC identici, in quanto questo indirizzo viene stabilito dal fornitore dell' hardware, la configurazione dell' host viene notevolmente semplificata. I primi 64 bit compongono

il cosiddetto `EUI-64` token, gli ultimi 48 bit vengono presi dall'indirizzo MAC ed i rimanenti 24 bit contengono particolari informazioni riguardanti il tipo di token (contrassegno). Questo consente di assegnare un `EUI 64` token anche a dispositivi senza indirizzo MAC (connessioni PPP ed ISDN!).

Da questa struttura di base derivano cinque tipi diversi di indirizzi unicast:

`::`(unspecified) Questo indirizzo viene utilizzato da un sistema come indirizzo sorgente quando la propria interfaccia di rete viene inizializzata per la prima volta e quindi non dispone ancora di alcuna informazione sul proprio indirizzo.

`::1` (loopback) Indirizzo del dispositivo di loopback.

Indirizzo compatibile con IPv4 L'indirizzo IPv4 e un prefisso di 96 zero bit all'inizio dell'indirizzo compongono l'indirizzo IPv6. Questo tipo di indirizzo di compatibilità viene utilizzato nel tunneling (si veda la sezione 22.2.3 nella pagina successiva). Gli host IPv4/IPv6 possono in tal modo comunicare con gli host che si trovano in una rete prettamente IPv4.

Indirizzo IPv4 mappato IPv6 Questo tipo di indirizzo indica un indirizzo IPv6 di un host IPv4.

Indirizzi locali Vi sono due tipi di indirizzi per l'uso prettamente locale:

link-local Questo tipo di indirizzo può essere utilizzato solamente nella sottorete locale. I router non inoltrano dei pacchetti con un indirizzo di destinazione o indirizzo sorgente di questo tipo né su Internet né su altre sottoreti. Questi indirizzi si distinguono per un prefisso particolare (`fe80::/10`) e l'ID di interfaccia della scheda di rete. La parte centrale dell' indirizzo è composto da zero byte che non indicano nulla di particolare. Questo tipo di indirizzo viene utilizzato durante il processo di configurazione automatica per indirizzare gli host della stessa sottorete.

site-local Questo tipo di indirizzo può essere instradato tra le varie sottoreti di una organizzazione (ingl.site) ma non su Internet. Questi indirizzi vengono utilizzati per Intranet, e sono un equivalente degli indirizzi privati dell'IPv4. Accanto ad un prefisso definito (`fec0::/10`) ed l'ID di interfaccia, questi indirizzi contengono un campo di 16 bit che codificano l'ID della sottorete. Il resto viene riempito con zero byte.

Inoltre, IPv6 presenta una novità: consente di assegnare ad una interfaccia di rete più indirizzi IP, in tal modo potrete accedere a diverse reti, di cui una può essere configurata in modo completamente automatico, prendendo un indirizzo MAC ed un prefisso noto, e dopo l'avvio di IPv6 grazie all' "indirizzo link local" potrete indirizzare direttamente tutti gli host all'interno della rete locale. Visto che l'indirizzo MAC è incluso nell'indirizzo IP, ognuno di questi indirizzi è unico in tutto il mondo. Solo le parti inerenti al *Site Topology* o *Public Topology* possono variare a seconda della rete di appartenenza dell'host.

Se un terminale si sposta tra reti differenti, gli servono almeno due indirizzi: uno è l' *home address* che contiene oltre all'ID di interfaccia delle informazioni inerenti alla sua rete home, dove viene utilizzato solitamente ed il relativo prefisso. L' *home address* è statico e non si modifica. Tutti i pacchetti inviati a questo indirizzo vengono consegnati sia nella propria rete che in quelle estranee. La consegna anche in reti estranee viene resa possibile grazie a delle innovazioni del protocollo IPv6, ovvero la *stateless autoconfiguration* e *neighbor discovery*. Il terminale mobile presenta accanto al suo indirizzo "home" ulteriori indirizzi appartenenti a delle ulteriori reti in cui si muove. Questi indirizzi hanno il nome di *care-of address*. Nella rete home del terminale mobile deve esservi una istanza che gli inoltra i pacchetti inviati al suo indirizzo "home", quando questi si trova in un'altra rete. In IPv6 questa funzione viene svolta da un *home agent* che inoltra tutti i pacchetti inviati all'indirizzo home (home address) del terminale mobile tramite un tunnel. I pacchetti con "care-of address" quale indirizzo di destinazione possono essere consegnati direttamente tramite l'home agent.

22.2.3 Coesistenza di IPv4 ed IPv6

Ce ne vorrà di tempo prima che tutti i sistemi presenti su Internet effettuino il passaggio da IPv4 a IPv6, così il vecchio ed il nuovo protocollo dovranno coesistere l'uno accanto all'altro. Questa coesistenza nel caso di un sistema è resa possibile grazie al *dual stack*. Resta comunque la questione del modo in cui sistemi IPv6 possano comunicare con sistemi IPv4, e del modo in cui realizzare il trasporto di pacchetti IPv6 attraverso reti IPv4 che al momento sono quelle maggiormente diffuse. Tunneling ed indirizzi di compatibilità (si veda la sezione 22.2.2 a pagina 407) sono gli approcci per affrontare questa questione.

Le reti IPv6, che al momento sono le meno diffuse, realizzano lo scambio di dati in reti IPv4 tramite cosiddetti tunnel. Nel tunneling i pacchetti IPv6 vengono racchiusi in pacchetti IPv4 per poter transitare in reti prettamente IPv4. Un tunnel connette due host IPv4. Per tale processo i pacchetti devono includere l'indirizzo

meta IPv6 (o il corrispondente prefisso) nonché l'indirizzo IPv4 del host remoto alla fine del tunnel. Nei casi più semplici gli amministratori di rete configurano *manualmente* dei tunnel tra le loro reti di compentenza. Questo metodo di tunneling viene definito tunneling *statico*.

Spesso il tunneling statico non basta per configurare ed amministrare la quantità di tunnel necessari per uno svolgimento senza intoppi del lavoro in rete. Per questo motivo sono stati ideati tre modi per realizzare il tunneling *dinamico*:

6over4 I pacchetti IPv6 vengono "integrati" automaticamente in pacchetti IPv4, ed inviati tramite una rete IPv4 con la funzionalità di multicasting abilitata. Ad IPv6 l'intera rete (Internet) "sembra" una LAN Local Area Network immensa. In tal maniera viene determinata in modo automatico l'estremità di destinazione IPv4 del tunnel. Lo svantaggio di questo approccio è da un lato dalla scarsa scalabilità ed il fatto che il multicasting IP non è affatto disponibile su tutto l'Internet. Questa soluzione è indicata per reti di piccole aziende o di istituzioni con il multicasting IP. L'RFC di riferimento è l'RFC2529.

6to4 Questo metodo consiste nel generare automaticamente indirizzi IPv4 da indirizzi IPv6. In tal maniera le poche reti IPv6, dette anche "isole IPv6", sparse nella Rete possono comunicare anche tramite una rete IPv4. Comunque, non è escluso l'insorgere di difficoltà durante lo scambio di dati tra reti IPv6 ed Internet. L'RFC di riferimento è l'RFC 3056.

IPv6 Tunnel Broker Qui dei server particolari creano i tunnel in modo automatico. L'RFC di riferimento è l' RFC 3053.

Importante

L'iniziativa 6Bone

Su Internet già "di vecchio stampo" troviamo *6Bone* (`http://www.6bone.net`), una rete dislocata composta da sottoreti IPv6 connesse per via di tunnel. All'interno della rete 6Bone viene testato IPv6. Fornitori di software e provider che sviluppano o offrono dei servizi IPv6 possono ricorrere a questo ambiente di test per raccogliere delle esperienze in merito. Per ulteriori informazioni consultate il sito di 6Bone.

Importante

22.2.4 Configurare IPv6

Se volete impostare IPv6 normalmente non dovete effettuare alcuna configurazione sulle postazioni di lavoro. E' però necessario caricare il supporto per IPv6; potete farlo eseguendo il comando `modprobe ipv6` come `root`.

Grazie all'approccio della configurazione automatica di IPv6, alla scheda di rete viene attribuito un indirizzo nella rete `link-local`. Normalmente, su una postazione di lavoro (workstation), non viene amministrata alcuna tabella di routing. La postazione di lavoro chiede ai router presenti nella rete, servendosi del *Router advertisment protocol*, quali siano il prefisso e i gateway da usare. Per configurare un router IPv6, potete utilizzare il programma radvd. Questo programma comunica alla workstation il prefisso da usare per gli indirizzi IPv6 e il/i router. Anche il programma zebra può venir utilizzato ai fini della configurazione di indirizzi e del routing.

Per configurare diversi tunnel ricorrendo ai file sotto `/etc/sysconfig/network` consultate la pagina di manuale di ifup (`man ifup`).

22.2.5 Ulteriore documentazione

Chiaramente quanto riassunto finora non è che una prima introduzione ad un tema così vasto come IPv6. Per degli approfondimenti in tema di IPv6, consultate la seguente documentazione che trovate online ed i seguenti manuali:

`http://www.ngnet.it/e/cosa-ipv6.php`
Una serie di articoli in cui vengono descritti i principi di IPv6. Indicato per un primo approccio a questo tema.

`http://www.bieringer.de/linux/IPv6/`
Linux-IPv6-HOWTO e tanti link.

`http://www.6bone.de/` Connettersi ad una rete IPv6 tramite un tunnel.

`http://www.ipv6.org/` Tutto in tema di IPv6.

RFC 2640 L'RFC introduttivo al tema IPv6.

IPv6 Essentials In inglese. Hagen, Silvia: *IPv6 Essentials*. O'Reilly & Associates, 2002. -(ISBN 0-596-00125-8).

22.3 Risoluzione dei nomi

Il DNS (Domain Name System) vi risparmia di dover tenere a mente gli indirizzi IP: grazie al DNS, un indirizzo IP viene assegnato ad uno o più nomi, e viceversa un nome viene assegnato ad un indirizzo IP. In Linux questo processo viene normalmente eseguito da un software speciale di nome bind. Il sistema che esegue questa conversione si chiama *server dei nomi*. I nomi sono disposti in un ordine gerarchico, e le singoli parti del nome sono divisi da punti. La gerarchia dei nomi, però, non dipende dalla gerarchia degli indirizzi IP sopra descritta.

Osserviamo da più vicino un nome completo, p.es. `laurent.suse.de` scritto nel formato `nomehost.dominio`. Un nome completo (in gergo "Fully qualified domain name" o *FQDN*) è composto dal nome del sistema accompagnato dal dominio (`suse.de`). Il dominio si compone di una parte liberamente scelta (nel nostro esempio: `suse` e di un cosiddetto *top level domain*, *TLD*. (`de`).

L'attribuzione dei TLD è un po' intricata. In America vengono p.es. usati TLD composti da 3 lettere, mentre nel resto del mondo vengono sempre usate le denominazioni ISO dei paesi, composte da due lettere. Dal 2000 vi sono inoltre ulteriori TLD per determinati settori con spesso più di tre lettere (p.es. `.info`, `.name`, `.museum` etc).

Agli albori di Internet (prima del 1990), esisteva a riguardo un file `/etc/hosts` in cui erano memorizzati i nomi di tutti i sistemi presenti su Internet. In breve tempo, a causa del numero sempre crescente dei computer collegati ad Internet, la cosa divenne impraticabile. Per questo venne creata una banca dati in grado di distribuire e memorizzare i nomi dei computer. Questa banca dati, appunto il server dei nomi sopra menzionato, non dispone dei dati di tutti i computer su Internet, ma delega le richieste ad altri server dei nomi che si trovano un gradino più basso nella gerarchia.

All'apice della gerarchia, si trovano i *root name server* che amministrano i top level domain. I server dei nomi root vengono amministrati dal network information center, ovvero *NIC*. Il server dei nomi root "conosce" i server dei nomi di competenza per un determinato top level domain. Nel caso del top level domain italiano `it` è l'IT-NIC ad essere preposto ai domini che terminano con il TLD `it`. Sulla pagina web `http://www.itnic.it` troverete ulteriori informazioni riguardanti l'IT-NIC; sul top level domain NIC troverete informazioni all'indirizzo `http://www.internic.net`.

DNS non risolve solo dei nomi di host, sa fare di più. Il server dei nomi, per esempio, "sa" anche quale sistema accetta le e-mail per tutto il dominio; si tratta del cosiddetto *Mail exchanger (MX)*.

Affinché il vostro computer sia in grado di risolvere un nome in un indirizzo IP, deve esservi almeno un server dei nomi con un indirizzo IP. La configurazione di un server dei nomi può essere eseguita comodamente con YaST. Se vi collegate tramite modem, può darsi che il protocollo usato per il collegamento fornisca l'indirizzo del server dei nomi durante il collegamento stesso. La configurazione dell'accesso al server dei nomi sotto SUSE LINUX viene descritta nel capitolo 24 a pagina 445.

Il protocollo `whois` è strettamente "imparentato" con DNS. Con l'omonimo programma whois, potrete scoprire velocemente quale server è l'istanza principale di un determinato dominio.

22.4 Configurare la connessione di rete tramite YaST

Il sistema deve disporre di una scheda rete supportata. Solitamente, la scheda di rete viene riconosciuta già durante l'installazione e il driver adatto viene integrato automaticamente. Potete vedere se la scheda è stata integrata correttamente dall'output del comando `ip address list eth0` che indica il dispositivo di rete `eth0`.

Se il supporto del kernel alla scheda di rete viene realizzato tramite un modulo – impostazione di default del kernel di –, allora bisogna indicare il nome del modulo in `/etc/sysconfig/hardware/hwcfg-*`. Se non c'è niente, `hotplug` seleziona automaticamente un driver. Non si distingue tra schede di rete atte all'hotplug e schede di rete integrate, `hotplug` seleziona un driver in ogni caso.

22.4.1 Configurare la scheda di rete con YaST

Dopo aver inizializzato il modulo di giungete ad una finestra di configurazione della rete. Nella parte superiore della finestra, sono elencate tutte le schede di rete da configurare. Se la vostra scheda non è stata riconosciuta correttamente durante il boot del sistema, sarà riportata con il suo nome in questo elenco. Dispositivi non rilevati vengono visualizzato come 'Altre (non riconosciute)'. Nella parte inferiore della finestra, appaiono invece le schede già configurate con tanto di tipo di rete ed indirizzo. Potete ora configurare una nuova scheda o modificare i parametri di dispositivi già configurati

La configurazione manuale della scheda di rete

Per configurare una scheda di rete non rilevata automaticamente, impostate i seguenti parametri:

Configurazione della rete Determinate il tipo di dispositivo dell'interfaccia e nome di configurazione. Selezionate il tipo di dispositivo tramite il combo box, il nome di configurazione potrete stabilirlo voi. Per la maggior parte dei casi si consiglia di applicare i valori di default. Per reperire delle informazioni sulla convenzione per i nomi di configurazione rimandiamo alla pagina di manuale di `getcfg`.

Modulo del kernel 'Nome della configurazione hardware' indica il nome del file `/etc/sysconfig/hardware/hwcfg-*` in cui sono archiviate le impostazioni hardware della vostra scheda di rete (ad es. nome del modulo del kernel appropriato). Le proposte di YaST per hardware PCMCIA e USB sono il più delle volte sensati. Negli altri casi: `0` è consigliabile solo se la scheda viene impostata con `hwcfg-static-0`.

Se la scheda di rete è un dispositivo PCMCIA o USB, abilitate i rispettivi check box e uscite dalla finestra con 'Prossimo'. Altrimenti selezionate tramite 'Seleziona dall'elenco' il modello della vostra scheda di rete. YaST selezionerà a questo punto il modulo del kernel adatto. Uscite dalla finestra con 'Prossimo'.

La configurazione dell'indirizzo di rete

Determinate il tipo di dispositivo dell'interfaccia e nome di configurazione. Selezionate il tipo di dispositivo tramite il combo box, il nome di configurazione potrete stabilirlo voi. Per la maggior parte dei casi si consiglia di applicare i valori di default. Per reperire delle informazioni sulla convenzione per i nomi di configurazione rimandiamo alla pagina di manuale di `getcfg`.

Se come tipo di dispositivo dell'interfaccia selezionate 'wireless', giungete alla prossima finestra 'Configurazione della scheda di rete wireless', dove potete configurare il modo operativo, nome di rete (ESSID) e cifratura. Con 'OK' concludete la configurazione della vostra scheda. Per una descrizione dettagliata della configurazione di schede WLAN rimandiamo alla sezione 17.1.3 a pagina 338. Per tutti gli altri tipi di interfaccia proseguite con il tipo di allocazione dell'indirizzo per la vostra scheda di rete:

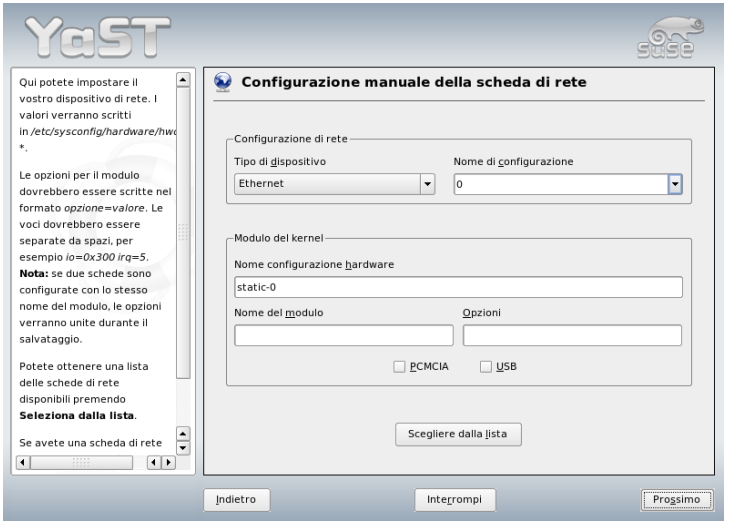

Figura 22.3: *Configurazione della scheda di rete*

'Allocazione automatica dell'indirizzo (con DHCP)'
Se la vostra rete comprende un server DHCP, potete farvi trasmettere da questo server i dati di configurazione della scheda di rete. Attivate anche l'allocazione indirizzo tramite DHCP se il vostro gestore DSL non vi ha comunicato un indirizzo IP statico. Con un DHCP, potete accedere al dialogo di configurazione del client con il pulsante 'Opzioni client DHCP'. Impostate se il server DHCP debba sempre rispondere ad un broadcast. Eventualmente, indicate anche un identificatore. Di default il sistema viene identificato in base all' indirizzo hardware della scheda di rete. Se utilizzate diverse macchine virtuali che utilizzano la stessa scheda di rete, potete distinguerle tramite diversi identificatori.

'Configurazione dell'indirizzo statico'
Se disponete di un indirizzo IP fisso, abilitate questa casella. Inserite l'indirizzo IP e la maschera di sottorete adatta alla vostra rete. Il valore preimpostato della maschera della sottorete è stato scelto in modo da rilevarsi sufficiente per una tipica rete domestica.

Per uscire da questo dialogo, cliccate su 'Prossimo' oppure impostate in alternativa il nome dell'host, il server dei nomi ed il routing (instradamento) (cfr. la a pagina 62 e la a pagina 64).

Tramite la casella 'Per esperti. . . ' potete eseguire delle impostazioni più complesse. Tra l'altro tramite 'Dettagli' potrete delegare il controllo sulla scheda di rete dall'amminstratore (`root`) all'utente normale, tramite appunto 'Amministrata dall'utente'. Se si lavora in diversi ambienti di rete questa impostazione consente all'utente di reagire in modo più flessibile se ci si trova di fronte a diversi tipi di connessione di rete, visto che può abilitare o disabilitare l'interfaccia. Inoltre, nella presente finestra potete stabilire l'MTU (Maximum Transmission Unit) e tipo di 'Abilitazione dispositivo'.

22.4.2 Modem

Nel centro di controllo di YaST, sotto 'Dispositivi di rete', troverete anche il modulo di configurazione per modem. Se il vostro modem non è stato rilevato automaticamente, impostatelo manualmente, specificando l'interfaccia alla voce 'Dispositivo modem' del dialogo di configurazione manuale.

Se il modem è connesso ad un impianto telefonico, avete bisogno di specificare il prefisso di composizione (di solito uno zero. Guardate nelle istruzioni d'uso del vostro impianto telefonico). Scegliete poi tra selezione a tono o a impulso, se accendere l'altoparlante o se aspettare il segnale di selezione (da evitare se il modem è allacciato ad una rete telefonica).

Sotto 'Dettagli' trovate le impostazioni del tasso di Baud e le stringhe di inizializzazione del modem. Impostate questi valori manualmente solo se il modem non è stato rilevato automaticamente e deve essere configurato per la trasmissione dati (specialmente nel caso dei terminal adapter ISDN). Per chiudere questo dialogo, cliccate su 'OK'. Se volete delegare il controllo sul modem all'utente normale sprovvisto dai permessi di root abilitate 'Amministrato dall'utente'. In tal modo l'utente può abilitare o disabilitare al momento opportuno. Tramite l'opzione 'Dial prefix regex' indicate un'espressione regolare a cui deve corrispondere il 'Prefisso di composizione' modificabile dall'utente normale in KInternet. Se il campo resta vuoto l'utente potrà impostare un diverso 'Prefisso di composizione' solo con i privileggi di root.

Selezionate l'ISP (Internet Service Provider). Se intendete selezionare il vostro provider dall'elenco degli provider predefiniti per il vostro paese, se il radio bottone 'Nazioni'. Alternativamente, cliccate su 'Nuovo' per giungere nel dialogo per l'impostazione manuale dei parametri ISP. Inserite il tipo di connessione nonché nome e numero di telefono del provider. Specificate anche il nome

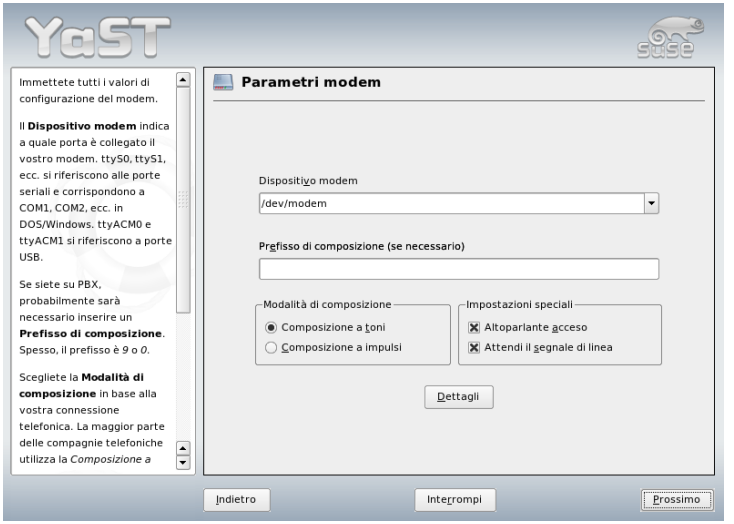

Figura 22.4: *Configurazione modem*

utente e password forniti dal provider. Attivate la casella 'Richiesta password' se preferite che vi venga chiesta la password ad ogni connessione.

Nell'ultimo dialogo, impostate i parametri di connessione:

'Dial-On-Demand' Indicate almeno un server dei nomi, se decidete di usufruire della funzione di dial-on-demand, ovvero connessione su richiesta.

'Modificare il DNS durante la connessione'
Normalmente, questa casella è attiva ed il server dei nomi viene adattato automaticamente ad ogni connessione. Disattivate questa opzione e specificate un server dei nomi fisso se avete scelto la 'Dial on Demand'.

'Rilevamento automatico del DNS' Se il provider non trasmettte il proprio domain name server dopo la connessione, disattivate questa opzione ed immettete i dati DNS manualmente.

'Modo "ignorance"' Questa è l'opzione abilitata di default. I prompt del del server dell'ISP vengono ignorati per non interferire con il processo di connessione.

'Attivare il firewall' Questa opzione attiva il firewall di che vi protegge da intrusioni durante il collegamento ad Internet.

'Interrompere dopo (secondi)' Impostate qui il numero di secondi dopo il quale il collegamento debba essere interrotto se non vi è più stata alcuna trasmissione di dati.

Dettagli IP Questo pulsante vi porta al dialogo di configurazione dell'indirizzo. Se il vostro provider non vi ha dato un indirizzo IP dinamico, disattivate la casella 'Indirizzo IP dinamico' e specificate sia l'indirizzo IP locale del vostro pc che l'indirizzo IP remoto. Se non li conoscete, chiedeteli al provider. La 'Default Route' resta attiva. Per chiudere il dialogo, cliccate su 'OK'.

Premete su 'Prossimo' e ritornerete nella finestra rassegna per vedere cosa avete configurato. Terminate l'impostazione con 'Fine'.

22.4.3 ISDN

Questo modulo vi permette di configurare una o più schede ISDN. Se la vostra scheda non viene riconosciuta automaticamente da YaST, dovrete configurarla manualmente. Teoricamente, potete configurare più di un'interfaccia, ma, per un utente domestico, ne basta una per configurare anche più provider. I dialoghi che seguono servono ad impostare i parametri necessari al funzionamento della scheda ISDN.

Segue una finestra (cfr. la figura 22.5 nella pagina successiva) 'Selezione del protocollo ISDN'. Il valore di default è 'Euro-ISDN (EDSS1)' (cfr. sotto caso 1 e 2a,). Per impianti telefonici più grandi ed obsoleti (cfr. caso 2b, sotto), usate '1TR6', per gli USA vale 'NI1'. L'abbreviazione del vostro paese la potete selezionare nel rispettivo box di selezione. Nel campo di immissione che si trova accanto potete indicare il prefisso (ad es. +39 per l'Italia) e il prefisso della vostra città nell'apposito campo (ad es. 06 per Roma). Se necessario, impostate anche prefisso di composizione.

Il dialogo di selezione del 'Modo di avviamento' vi permette di impostare il modo di avviamento della scheda ISDN. 'OnBoot' significa che il driver ISDN viene inizializzato all'avvio del sistema. Se scegliete l'opzione 'Manuale', dovrà essere l'utente ad inizializzare il driver con il comando `rcisdn start`. Con l'opzione 'Hotplug', invece, il driver si inizializza quando viene connessa la scheda PCMCIA o il dispositivo USB. Conclusa la fase di configurazione, premete 'Ok'.

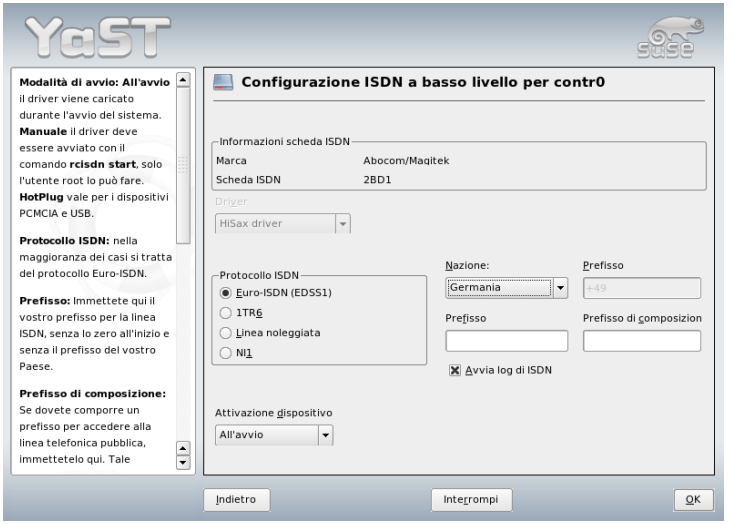

Figura 22.5: *Configurazione ISDN*

Nel prossimo dialogo, definite l'interfaccia della vostra scheda ISDN od ulteriori provider per un' interfaccia esistente. Le interfacce possono avere il modo operativo `SyncPPP` o `RawIP`: la maggior parte dei gestori usano `SyncPPP`, che vi descriveremo di seguito.

Per 'Numero di telefono proprio', le indicazioni dipendono dal vostro scenario:

La scheda ISDN è connessa direttamente alla presa telefonica
L'ISDN vi offre, di solito, tre numeri telefonici (MSN Multiple Subscriber Number), ma su richiesta si arriva anche a dieci. In questo dialogo, dovete attribuire uno dei numeri MSN alla vostra scheda ISDN. Digitatelo senza prefisso. Se sbagliate numero, il gestore della rete utilizzeràil primo MSN attribuito al vostro allacciamento ISDN.

La scheda ISDN è connessa ad un impianto telefonico
A seconda dei casi, sono necessari diversi parametri:

1. Gli impianti telefonici domestici utilizzano solitamente il protocollo Euro-ISDN/EDSS1 per gli allacci interni. Questi impianti hanno un

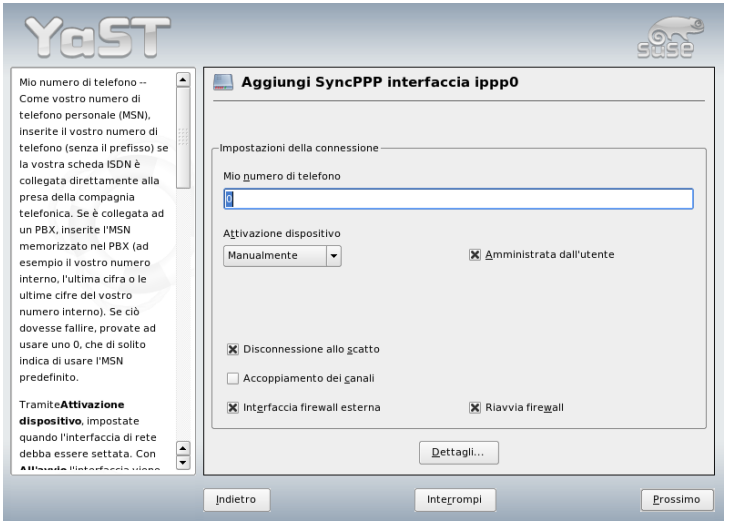

Figura 22.6: *Configurazione dell'interfaccia ISDN*

S0-Bus interno ed usano numeri di telefono interni per gli apparecchi connessi all'impianto.

Come MSN, usate uno dei numeri di telefono interni. Uno degli MSN del vostro impianto dovrebbe funzionare se è abilitato l'accesso dall'esterno. Altrimenti, provate con uno zero. Per maggiori dettagli, consultate la documentazione relativa al vostro impianto telefonico.

2. Per le aziende: nel caso di impianti telefonici di notevoli dimensioni si ricorre di solito al protocollo 1TR6 per gli allacci interni. In questo caso, l'MSN si chiama EAZ ed è il suffisso di selezione interna. Per la configurazione Linux, basta indicare solo l'ultima cifra dell'EAZ. Nel peggior dei casi provate con le cifre da 1 a 9.

Potete determinate se desiderate l'interruzione automatica della connessione prima che vi sia il prossimo scatto ('ChargeHUP'). Questa opzione non funziona con tutti i provider. Se desiderate un 'Raggruppamento dei canali' (Multilink PPP), attivatene la casella. Se desiderate attivare il SuSEfirewall2, selezionate la casella 'Attiva firewall'. Per dare la possibilità all'utente normale di abilitare o disabilitare l'interfaccia, selezionate la voce 'Amministrata dall'utente'.

Il pulsante 'Dettagli' apre un dialogo di configurazione per scenari di una certa complessità che non riguardano da vicino l'utente medio domestico. Per chiudere il dialogo, cliccate su 'Prossimo'.

Il dialogo successivo serve all'impostazione dell'allocazione dell'indirizzo IP. Se il vostro provider non vi ha dato alcun indirizzo IP, selezionate 'Indirizzo IP dinamico'. Altrimenti, inserite l'indirizzo IP locale del vostro computer e l'indirizzo IP remoto che vi ha fornito il provider. Se l'interfaccia da configurare deve essere la route standard per Internet, attivate la casella 'Standard route'. Attenzione: ogni sistema vuole solo un'unica interfaccia come standard route. Chiudete il dialogo con 'Prossimo'.

Nel dialogo successivo, impostate nazione e provider. I gestori della lista sono solo call-by-call. Se il vostro provider non è nella lista, cliccate su 'Nuovo'. Appare la maschera 'Parametri ISP', in cui eseguire le impostazioni del caso. Il numero di telefono non può contenere virgole o spazi. Dopodiché, inserite il vostro nome utente e la password. Cliccate poi su 'Prossimo'.

Per utilizzare 'Dial on demand' su una postazione monoutente, dovrete configurare il DNS (server dei nomi). La maggior parte dei provider supportano l'attribuzione dinamica del DNS, il che vuol dire che, alla creazione della connessione viene trasmesso l'indirizzo IP attuale del server dei nomi. Nel vostro sistema, dovrete tuttavia impostare un DNS server posticcio, come `192.168.22.99`. Se non avete ricevuto un'attribuzione dinamica dal server dei nomi, inserite qui l'indirizzo IP del server dei nomi del vostro provider. Inoltre, in questo dialogo, potete impostare il numero di secondi al trascorrere del quale il collegamento debba venire interrotto, se non vi è una trasmissione di dati. Confermate le vostre impostazioni con 'Prossimo' ed arrivate ad un elenco delle interfacce. Attivate le vostre impostazioni con 'Fine'.

22.4.4 Modem via cavo

In alcuni paesi (Austria, USA), il collegamento Internet avviene tramite la rete della televisione via cavo. L'abbonato riceve un modem dal gestore della rete e connette il modem al cavo del televisore, da una parte, e, dall'altra, alla scheda di rete del computer con un cavo 10Base-T (Twisted-Pair). Questo tipo di modem per il computer rappresenta una linea fissa con indirizzo IP fisso.

Leggete le istruzioni del vostro provider e scegliete tra 'Allocazione automatica dell'indirizzo (con DHCP)' e 'Configurazione dell'indirizzo statico'. La maggior parte dei gestori, al giorno d'oggi, usa il DHCP. L'indirizzo IP statico viene più

che altro impiegato in ambito dell'offerte rivolte all'utenza business del provider. Il provider ha in questi casi un indirizzo IP fisso.

Vi invitiamo a leggere anche gli articoli della banca dati di supporto sull'installazione e la configurazione dei modem via cavo, all'indirizzo:`http://
/portal.suse.com/sdb/en/2002/06/cmodem8.html`

22.4.5 DSL

Per configurare la connessione DSL vi è il modulo 'DSL' sotto 'Dispositivi di rete'. Scorrendo diverse finestre avete modo di inserire i dati specifici per il vostro accesso DSL. vi permette di configurare l'accesso DSL basato sui seguenti protocolli:

- PPP over Ethernet (PPPoE) - Germania
- PPP over ATM (PPPoATM) - Inghilterra
- CAPI per ADSL (schede Fritz)
- Protocollo tunnel per Point-to-Point (PPTP) - Austria

Tenete presente che la configurazione del vostro accesso DSL tramite PPPoE e PPTP presuppone la corretta configurazione della vostra scheda di rete. Se dovete ancora provvedere, proseguite con 'Configurare schede di rete' (si veda la sezione 22.4.1 a pagina 415). L'allocazione automatica degli indirizzi IP con DSL non avviene tramite il protocollo DHCP. Quindi non potete ricorrere a 'Allocazione automatica degli indirizzi (tramite DHCP)'. Assegnate invece un indirizzo IP dummy statico, del tipo. `192.168.22.1`. Nel campo 'Maschera di sottorete' inserite `255.255.255.0`. Nel caso di una postazione di lavoro monoutente lasciate assolutamente vuoto il campo 'Gateway di default'.

Suggerimento

I valori per 'Indirizzo IP' del vostro sistema e 'Maschera di sottorete' sono solo dei segnaposto. Non sono rilevanti per la creazione del collegamento, servono solo all' abilitazione della scheda di rete.

Suggerimento

All'inizio della configurazione (si veda figura 22.7 nella pagina successiva), selezionate il modo PPP e la scheda Ethernet alla quale è connesso il vostro modem

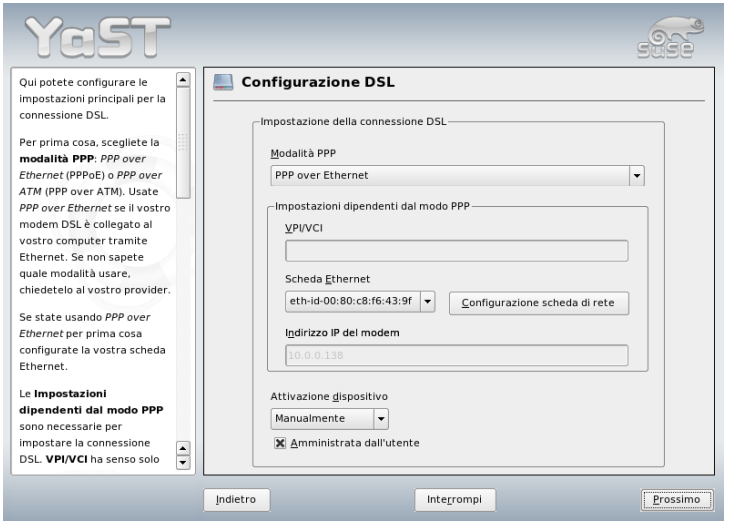

Figura 22.7: *Configurazione del DSL*

(di solito, il parametro è `eth0`). Nel dialogo 'Attivazione dispositivi', impostate se il vostro sistema debba connettersi già all'avvio o successivamente. Tramite 'Amminstrata dall'utente' l'utente normale potrà abilitare e disabilitare l'interfaccia, senza che siano richiesti i privileggi di root, tramite KInternet. Dopodiché, selezionate la vostra nazione ed il provider. Il contenuto dei dialoghi che seguono dipende dai parametri già inseriti. Per maggiori dettagli, consultate i testi di aiuto dei dialoghi.

Per utilizzare 'Dial on demand' in un sistema monoutente, dovrete configurare il DNS (server dei nomi). La maggior parte dei provider supportano l'attribuzione dinamica del DNS, il che vuol dire che, il programma trasmette l'attuale indirizzo IP del server dei nomi all'inizio della connessione. Nel vostro sistema, dovrete tuttavia impostare un DNS server posticcio, come `192.168.22.99`. Se non avete ricevuto un'attribuzione dinamica del name server, inserite qui l'indirizzo IP del name server del vostro provider.

Interessante è anche la casella 'Interrompi connessione dopo (secondi)', in cui potete determinare per quanto tempo il sistema debba restare connesso dopo l'ultimo transfer di dati. Vi consigliamo un valore tra i 60 e i 300 secondi. Nel

caso del 'Dial-On-Demand' si consiglia di disattivare la funzione automatica di interruzione della connessione, impostando il valore di 0 secondi.

Per la configurazione di T-DSL procedete attenendovi a quanto già illustrato per DSL. Selezionando 'T-Online' quale Provider raggiungete automaticamente la finestra di configurazione per T-DSL. I dati richiesti: identificativo linea, codice T-Online, shared user ID e la vostra password. Questi dati vi vengono forniti dal vostro provider.

22.5 Configurazione manuale della rete

La configurazione manuale della rete dovrebbe sempre essere la seconda scelta. Noi consigliamo di usare YaST. Una illustrazione dei concetti che stanno alla base della configurazione di rete, semplificherà l'utilizzo di YaST.

Ogni scheda di rete — indipendentemente se integrata o un dispositivo hotplug (PCMCIA, USB, a volte anche PCI) — viene rilevata e configurata dal sistema hotplug. Per comprendere questo processo bisogna sapere che: una scheda di rete compare nel sistema in due modi differenti. Una volta come *dispositivo* (ingl. device) fisico, e dall'altra come *interfaccia* (ingl. interface). Se viene inserito e rilevato un dispositivo del genere si ha un evento hotplug che inizializza il dispositivo tramite lo script `/sbin/hwup`. Inizializzando la scheda di rete come nuova interfaccia di rete, il kernel crea un ulteriore evento di hotplug che innesca la configurazione dell' interfaccia tramite `/sbin/ifup`.

Il kernel numera i nomi di interfaccia nell'ordine in cui sono state registrate. La sequenza di inizializzazione è determinante ai fini dell'assegnazione del nome. Se disponete di diverse schede di rete e la prima nella sequenza viene rimossa o non reagisce più cambia anche la numerazione delle schede inizializzate dopo quella in questione. Con schede hotplug "vere" è determinante la sequenza nella quale sono stati connessi i dispositivi.

Per consentire una configurazione flessibile è stato distinto tra configurazione del dispositivo (hardware) e dell'interfaccia ed inoltre l'allocazione delle configurazioni ai dispositivi o interfacce non viene più realizzata tramite i nomi delle interfacce. Le impostazioni dei dispositivi si trovano sotto `/etc/sysconfig/hardware/hwcfg-*`, mentre le impostazioni per le interfacce si trovano sotto `/etc/sysconfig/network/ifcfg-*`. I nomi dei file di configurazione sono scelti in modo da descrivere i dispositivi o interfacce a cui fanno riferimento. Visto che prima l'allocazione tra driver e nomi di interfacce presupponeva nomi di interfaccia costanti, l'allocazione non può più avvenire tramite

`/etc/modprobe.conf`. Con il nuovo approccio le registrazioni alias in questo file comporterebbero addirittura degli effetti collaterali indesiderati.

I nomi di configurazione, dunque la parte che segue dopo `hwcfg-` o `ifcfg-` possono indicare il punto di connessione, un ID specifico del dispositivo o anche il nome dell'interfaccia. Nel caso di una scheda PCI si avrebbe una designazione del tipo `bus-pci-0000:02:01.0` (slot PCI) o `vpid-0x8086-0x1014-0x0549` (ID del fornitore e prodotto). Per la relativa interfaccia si potrebbe utilizzare anche `bus-pci-0000:02:01.0` oppure `wlan-id-00:05:4e:42:31:7a` (indirizzo MAC).

Se non si vuole assegnare una determinata configurazione di rete a una scheda determinata ma a una scheda qualunque di un certo tipo (di cui è inserita sempre una sola alla volta), si sceglie un nome di configurazione più generale; ad esempio si può utilizzare `bus-pcmcia` per tutte le schede PCMCIA, oppure si possono delimitare i nomi anteponendo un tipo di interfaccia, ad esempio `wlan-bus-usb` verrebbe assegnata a tutte le schede WLAN connesse ad una porta USB.

Valgono sempre quelle impostazioni che meglio descrivono l'interfaccia o il dipositivo messo a disposizione dall'interfaccia. É `/sbin/getcfg` a stabilire la miglior configurazione. L'output di `getcfg` indica tutte le informazioni riguardanti la descrizione di un dispositivo. La specificazione per i nomi di configurazione è reperibile nella pagina di manuale di `getcfg`.

Seguendo il metodo illustrato si può impostare l'interfaccia di rete con la configurazione giusta, anche se i dispositivi di rete non vengono inizializzati sempre nella stessa sequenza. Rimane comunque il problema che il nome dell'interfaccia dipende dalla sequenza di inizializzazione. Vi sono due modi per accedere in modo affidabile all'interfaccia di una determinata scheda di rete:

- Tramite `/sbin/getcfg-interface` ⟨*`nome_di_configurazione`*⟩ si ottiene il nome della rispettiva interfaccia di rete; ciò consente di inserire in alcuni (purtroppo non ancora in tutti) file di configurazione di servizi di rete il nome di configurazione (ad es. firewall, `dhcpd`, routing, diverse interfacce di rete virtuali (tunnel)) al posto del nome di interfaccia (che non è persistente).
- Per interfacce la cui configurazione non porta il nome dell'interfaccia, è possibile assegnare un nome di interfaccia persistente tramite l'immissione di `PERSISTENT_NAME=<nomep>` in una configurazione di interfaccia (`ifcfg-*`). Il nome persistente ⟨*nomep*⟩ non può essere identico a quello che verrebbe assegnato automaticamente dal kernel, quindi non sono consentiti indicazioni del tipo `eth*`, `tr*`, `wlan*`, `qeth*`,

iucv* etc. Si propongono a tal fine invece designazioni del tipo net* o nomi parlanti come esterno, interno oppure dmz. I nomi persistenti vengono assegnati all'interfaccia solo dopo la sua registrazione, cioé il driver della scheda di rete deve essere caricato nuovamente (o invocate hwup <descrizione_del_dispositivo>) . A tal fine non basta un rcnetworkrestart.

Importante

Utilizzare nomi di interfaccia persistenti

Considerate che l'uso di nomi persistenti non è stato testato a fondo. Può verificarsi il caso che determinate applicazioni non riescano a maneggiare nomi di interfaccia stabiliti liberamente. In questi casi, rivolgetevi (preferibilmente in inglese) a http://www.suse.de/feedback.

Importante

ifup non inizializza l'hardware ma presuppone un'interfaccia preesistente. Per inizializzare l'hardware vi è hwup che viene invocato da hotplug (o coldplug). Non appena si inizializza un dispositivo viene però invocato automaticamente ed eventualmente settato ifup per la nuova interfaccia tramite hotplug se il modo di avvio è impostato su onboot, hotplug o auto ed è stato avviato il servizio network. Prima era un ifup <nomeinterfaccia> a inizializzare l'hardware. Ora si procede proprio in maniera inversa. Prima viene inizializzato una componente hardware e ne conseguono tutta una serie di azioni. Così è possibile impostare in maniera ottimale un numero variabile di dispositivi con un dato set di configurazioni.

Per una panoramica più articolata, la seguente tabella indica gli script che entrano in gioco durante il processo di configurazione della rete. Quando possibile è stato distinto tra aspetti che interessano l'hardware e quelli che riguardano più da vicino l'interfaccia:

Tabella 22.5: Gli script per configurare manualmente la rete

Fase di configurazione	Comando	Funzionalità
Hardware	`hw{up,down,status}`	Gli script `hw*` vengono invocati dal sottosistema hotplug per inizializzare un dispositivo, interrompere l'inizializzazione o per visualizzare lo stato di uno dispositivo. Per maggiori informazioni rimandiamo a `man hwup`.
Interfaccia	`getcfg`	Con `getcfg` ottenete il nome di interfaccia relativa al nome di configurazione o descrizione hardware. Per maggiori informazioni rimandiamo a `man getcfg`.
Interfaccia	`if{up,down,status}`	Gli script `if*` attivano o disattivano interfacce preesisteni o ritornano lo stato dell'interfaccia in questione. Per maggiori informazioni rimandiamo a `man ifup`

Per ulteriori indicazioni in tema di *Hotplug* e *Nomi di dispositivi persistenti* consultate il capitolo 18 a pagina 359 e capitolo 19 a pagina 367.

22.5.1 File di configurazione

Questa sezione riassume i file di configurazione di rete e spiega la loro funzione ed il formato utilizzato.

/etc/syconfig/hardware/hwcfg-*

Questi file contengono la configurazione hardware delle schede di rete e altri dispositivi; contengono inoltre i parametri necessari come modulo del kernel, modo di avviamento e script assegnati. Per maggiori dettagli consultate le pagine di manuale di `hwup`. Le impostazioni in `hwcfg-static-*` vengono applicate all'avvio di coldplug, indipendentemente dall'hardware presente.

/etc/sysconfig/network/ifcfg-*

Questi file contengono le impostazioni per le interfacce di rete. Includono tra le altre cose il modo di avvio e l'indirizzo IP. I parametri consentiti sono descritti nella pagina di manuale di `ifup`. É inoltre possibile utilizzare nei file `ifcfg-*` tutte le variabili contenute nei file di `dhcp`, `wireless` e `config`, se una impostazione altrimenti generale debba essere applicata ad una sola interfaccia.

/etc/sysconfig/network/config,dhcp,wireless

Il file `config` contiene impostazioni generali per il comportamento di `ifup`, `ifdown` e `ifstatus` che sono ben commentate. Troverete anche commenti in `dhcp` e `wireless`, dove risiedono le impostazioni generali per DHCP e schede di rete wireless. Tutte le variabili di questi file possono essere utilizzate anche in `ifcfg-*`, e hanno lì la precedenza.

/etc/sysconfig/network/routes,ifroute-*

Qui stabilite il routing statico di pacchetti TCP/IP. Tutte le route statiche richieste dai vari task di sistema possono essere immesse nel file `/etc/sysconfig/network/routes`: delle route per un host, per un host tramite gateway e route per una rete. Per ogni interfaccia è richiesto un routing specifico, impostate un ulteriore file di configurazione: `/etc/sysconfig/network/ifroute-*`. Al posto di * inserite il nome dell'interfaccia. Le registrazioni nel file di configurazione del routing assumono il seguente aspetto:

```
DESTINATION           GATEWAY NETMASK   INTERFACE [ TYPE ] [ OPTIONS ]
DESTINATION           GATEWAY PREFIXLEN INTERFACE [ TYPE ] [ OPTIONS ]
DESTINATION/PREFIXLEN GATEWAY -         INTERFACE [ TYPE ] [ OPTIONS ]
```

Se volete omettere GATEWAY, NETMASK, PREFIXLEN o INTERFACE, utilizzate al loro posto un `-`. Potete anche omettere le voci TYPE ed OPTIONS.

Nella prima colonna vi è la destinazione della route (un indirizzo IP di una rete o host oppure nel caso di server dei nomi *indirizzabili* il nome completo della rete o dell'host.

La seconda colonna indica il gateway di default o un gateway attraverso il quale un host o una rete può essere indirizzata. Nella terza colonna abbiamo la maschera di rete per reti o host dietro un gateway (ecco una maschera per un host dietro un gateway `255.255.255.255`)

L'ultima colonna è rilevante solo per reti connesse all'host locale, come ad es. loopback, ethernet, ISDN, PPP e dispositivi cosiddetti dummy. Qui va immesso il nome di dispositivo.

/etc/resolv.conf

Qui si indica a quale dominio appartenga l'host (parola chiave `search`) e quale sia l'indirizzo del server dei nomi (parola chiave `nameserver`) da indirizzare. Possono venire indicati più di un nome di dominio. Al momento della risoluzione di un nome non del tutto qualificato si cercherà di creare un nome valido e completamente qualificato ricorrendo alle registrazioni in `search`. Diversi server dei nomi possono venir resi noti tramite più righe inizianti con `nameserver`. I commenti vengono introdotti da # YaST registra qui il server dei nomi indicato.

Esempio 22.5: `/etc/resolv.conf`

```
# Il nostro dominio
search
#
# Usiamo  () come server dei nomi
nameserver
```

Alcuni servizi, come `pppd` (`wvdial`), `ipppd` (`isdn`), `dhcp` (`dhcpcd` e `dhclient`), `pcmcia` e `hotplug` modificano il file `/etc/resolv.conf` tramite lo script `modify_resolvconf`.

Una volta modificato temporaneamente il file `/etc/resolv.conf` attraverso questo script, esso conterrà un commento definito che dichiarerà da che tipo di servizio è stato modificato, dove è memorizzato il file originale, e come possono essere disattivate le modifiche automatiche. Se `/etc/resolv.conf` è stato modificato più volte, questa concatenazione di modifiche verrà sempre disattivata in modo ordinato, anche se le modifiche vengono annullate in ordine sparso. Cosa che può tranquillamente accadere, nel caso di `isdn`, `pcmcia` e `hotplug`.

Se avete terminato un servizio in modo non corretto, è possibile ripristinare lo stato iniziale con `modify_resolvconf`. Durante il caricamento, il sistema verifica se si sia fermato un `resolv.conf` modificato (p.es. a causa di un crollo del sistema) per poi ripristinare la versione originale (non modificata) di `resolv.conf`

`modify_resolvconf check`, permette a YaST di stabilire se `resolv.conf` sia stato modificato ed avvertire l'utente che tali modifiche andranno perse con il ripristino della versione originale. Altrimenti non si serve di `modify_resolvconf`: modifiche apportate al file `resolv.conf` tramite ed una modifica effettuata manualmente sono equivalenti. In entrambi i casi, si tratta di una modifica mirata e duratura, mentre le modifiche tramite uno dei servizi menzionati sono di natura temporanea.

/etc/hosts

In questo file (si veda l'esempio 22.6 in questa pagina) vengono assegnati gli indirizzi IP agli host. Se non si utilizzano server dei nomi, devono venire elencati tutti gli host con i quali deve venire creato un collegamento IP. Per ogni host, in questo file viene annotata una riga consistente dell' indirizzo IP, nome qualificato e nome dell'host (p.es.). L'indirizzo IP deve trovarsi all'inizio della riga, le registrazioni vengono separate da spazi o da tabulazioni. I commenti vengono preceduti da #.

Esempio 22.6: `/etc/hosts`

```
127.0.0.1 localhost
192.168.0.20 sole.example.com sole
192.168.0.1 terra.example.com terra
```

/etc/networks

Qui vengono convertiti i nomi della rete in indirizzi di rete. Il formato assomiglia a quello del file `hosts`, qui però i nomi della rete precedono gli indirizzi (si veda l'esempio 22.7 in questa pagina).

Esempio 22.7: `/etc/networks`

```
loopback     127.0.0.0
localnet     192.168.0.0
```

/etc/host.conf

La risoluzione dei nomi, cioè la traduzione di nomi di host o di reti tramite la libreria *resolver* viene controllata da questo file; questo file viene usato solo per programmi linkati con libc4 o libc5; per i programmi glibc attuali, si veda le impostazioni in `/etc/nsswitch.conf`! Ogni parametro deve trovarsi in una propria riga, commenti vengono introdotti da #. La tabella 22.6 a fronte mostra i parametri possibili.

Tabella 22.6: *Parametri per /etc/host.conf*

order *hosts*, *bind*	Sequenza nella quale vengono usati i servizi per la risoluzione di un nome. Possibili argomenti sono (separati da uno spazio o virgola): *hosts*: cercare nel file `/etc/hosts` *bind*: uso di un server dei nomi *nis*: tramite NIS
multi *on*/*off*	Determina se un host registrato in `/etc/hosts` possa avere più indirizzi IP.
nospoof *on* spoofalert *on*/*off*	Questi parametri influiscono su lo *spoofing* del server dei nomi, ma non influiscono sulla configurazione della rete.
`trim domainname`	Il nome del dominio indicato viene distaccato dal nome di host prima la risoluzione del nome (sempre che il nome dell'host contenga questo nome di dominio). Questa opzione è d'aiuto se nel file `/etc/hosts` esistono solo nomi del dominio locale che però devono venire riconosciuti anche col nome del dominio annesso.

Esempio 22.8: *`/etc/host.conf`*

```
# We have named running
order hosts bind
# Allow multiple addrs
multi on
```

/etc/nsswitch.conf

Con la GNU C Library 2.0 è arrivato anche il *Name Service Switch* (NSS) (si veda `man 5 nsswitch.conf`), come pure per maggiori dettagli *The GNU C Library Reference Manual*, il capitolo "System Databases and Name Service Switch".

Il file `/etc/nsswitch.conf` stabilisce la sequenza nella quale verranno richieste determinate informazioni. Un esempio per `nsswitch.conf` viene mostrato

nell'esempio 22.9 in questa pagina. I commenti vengono introdotti da #. In questo caso per esempio, la registrazione nella banca dati `hosts` significa che una richiesta viene inviata a `/etc/hosts` (`files`) tramite DNS (si veda il capitolo 24 a pagina 445)).

Esempio 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
```

Le banche dati disponibili tramite NSS sono indicate nella tabella 22.7 in questa pagina; in futuro ci saranno anche `automount`, `bootparams`, `netmasks` e `publickey`. Banche dati disponibili tramite /etc/nsswitch.conf sono elencate in tabella 22.8 a fronte.

Tabella 22.7: *Banche dati disponibili tramite /etc/nsswitch.conf*

`aliases`	Alias di mail, usato da `sendmail`; si veda `man 5 aliases`.
`ethers`	Indirizzi ethernet.
`group`	Usato da `getgrent` per gruppi di utenti; si veda `man group` .
`hosts`	Usato da `gethostbyname` e funzioni simili per nomi host e indirizzi IP.
`netgroup`	Elenco valido nella rete di host e utenti per regolare i diritti d'accesso; si veda la `man 5 netgroup`.
`networks`	Nomi ed indirizzi di rete usati da `getnetent`
`passwd`	Password degli utenti usate da `getpwent`; si veda la pagina di manuale `man 5 passwd`.

`protocols`	Protocolli di rete usati da `getprotoent`; si veda la pagina di manuale `man 5 protocols`.
`rpc`	Nomi e indirizzi per la "Remote Procedure Call" usati da `getrpcbyname` e funzioni simili.
`services`	Servizi di rete usati da `getservent`.
`shadow`	Password "shadow" degli utenti usate da `getspnam`; si veda la pagina di manuale `man. 5 shadow`.

Tabella 22.8: *Opzioni di configurazione delle banche dati NSS*

`files`	Accesso diretto ai file, per esempio su `/etc/aliases`.
`db`	Accesso tramite una banca dati.
`nis`	Si veda il capitolo 25 a pagina 467.
`dns`	Da usare come estensione solo con `hosts` e `networks`.
`compat`	Da usare come estensione solo con `passwd`, `shadow` e `group`

/etc/nscd.conf

Tramite questo file viene configurato l'nscd (ingl. Name Service Cache Daemon); si veda `man 8 nscd` e `man 5 nscd.conf`. Di default le voci in `passwd` e `groups` vengono tenute nella cache. Per servizi di directory come NIS e LDAP ciò contribuisce in modo essenziale ad un buon livello di prestazione, poiché altrimenti per ogni accesso a nomi e gruppi si dovrebbe realizzare una connessione di rete. `hosts` di solito non viene memorizzato temporaneamente (chaching), dato che il sistema non può più fare affidamento su "forward/reverse lookups" di questo servizio di nome. Invece di affidare tale compito all' nscd, si dovrebbe impostare un server dei nomi "caching".

Se, per esempio, è attivo il caching per `passwd`, ci vogliono in genere 15 secondi fino a che un utente locale appena creato sia noto al sistema. Riavviando nscd, si può ridurre il tempo d'attesa, il comando sarebbe: `rcnscdrestart`

/etc/HOSTNAME

Qui si trova il nome dell'host, cioè solo il nome dell'host senza il nome del dominio. Durante l'avvio del computer, questo file viene letto da diversi script; il file può contenere solo una riga recante il nome dell'host!

22.5.2 Script di inizializzazione

Oltre ai file di configurazione descritti esistono diversi script che durante l'avvio del computer, inizializzano i programmi di rete. Questi script vengono avviati non appena il sistema passa in uno dei *runlevel multiutente*, (si veda la tabella 22.9 in questa pagina).

Tabella 22.9: *Alcuni script di inizializzazione dei programmi di rete*

`/etc/init.d/network`	Questo script si occupa della configurazione delle interfacce di rete. L'hardware deve essere già stata inizializzata tramite `/etc/init.d/coldplug` (tramite `hotplug`). Se non è stato lanciato il servizio `network` le interfacce di rete non potranno essere settate dal sistema hotplug al loro inserimento.
`/etc/init.d/inetd`	Lancia l'xinetd a cui si può ricorrere per mettere a disposizione all'occorrenza dei servizi di sistema sul sistema; ad es. può lanciare vsftpd non appena viene inizializzata una connessione FTP.
`/etc/init.d/portmap`	Lancia il port mapper che è necessario per poter usare i server RPC, come ad esempio un server NFS.
`/etc/init.d/nfsserver`	Inizializza il server NFS.
`/etc/init.d/postfix`	Controlla il processo sendmail.
`/etc/init.d/ypserv`	Lancia il server NIS.
`/etc/init.d/ypbind`	Lancia il client NIS.

22.6 smpppd come assistente di selezione

La maggioranza degli utenti domestici non è collegata perennemente ad Internet, ma vi si collega all'occorrenza. Questo collegamento viene controllato a secondo del tipo di collegamento (ISDN o DSL) da ipppd o da pppd. In linea di massima è sufficiente avviare correttamente questi programmi per essere online.

Se avete un canone fisso (flat-rate) grazie al quale non vi vengano addebbitati dei costi aggiuntivi per creare la connessione, è sufficiente avviare correttamente il demone (deamon). Spesso comunque si desidera controllare il collegamento tramite un applet, ovvero un miniprogramma, di KDE oppure tramite un'interfaccia da linea di comando. Inoltre, spesso l'internet gateway è un altro computer rispetto alla postazione di lavoro effettivamente utilizzata, e così ci si ritrova a dover monitorare il collegamento ad Internet tramite un host di rete.

Ed è qui che entra in gioco smpppd (meta PPP-daemon) che mette a disposizione alle utility una interfaccia uniforme che funziona in entrambi le direzioni. Da una parte effettua la programmazione del rispettivo pppd o ipppd necessario e controlla il processo di selezione. Inoltre mette a disposizione ai programmi utenti diversi provider e trasmette delle informazioni sullo stato attuale del collegamento. Dato che si può gestire smpppd anche via rete, si adatta particolarmente alla gestione delle connessioni ad Internet da una postazione di lavoro con una propria sottorete privata.

22.6.1 Configurare smpppd

Le connessioni messe a disposizione da smpppd vengono configurate automaticamente da YaST. I programmi con cui si va effettivamente su Internet come kinternet e cinternet sono già preconfigurati. Si deve intervenire manualmente solo se si vogliono impostare ulteriori feature di smpppd, come la gestione da remoto.

Il file di configurazione di smpppd si trova sotto `/etc/smpppd.conf`. Di default non è abilitato il controllo da remoto. Tra le opzioni di maggior interesse di questo file di configurazione vi sono:

open-inet-socket = <yes | no> Se volete amministrare smpppd via rete, questa opzione deve essere impostata su `yes`. La porta su cui smpppd si mette in ascolto è `3185`. Se questo parametro è impostato su `yes`, dovreste impostare di conseguenza anche i parametri `bind-address`, `host-range` e `password`.

bind-address = <ip> Se un computer ha diversi indirizzi IP tramite questo parametro si può stabilire l'indirizzo IP per il quale smpppd debba accettare delle richieste di connessione.

host-range = <min ip> <max ip> Il parametro `host-range` definisce un'area di rete. Gli host con un indirizzo IP all'interno di questo intervallo hanno il permesso di accedere a smpppd. Agli host che non si trovano in questa area, l'accesso viene negato.

password = <password> Impostando una password si restringe l'accesso dei client ai soli host con autorizzazione. Visto che comunque si tratta di una password non cifrata, non sopravvalutatene l'efficacia in termini sicurezza. Se non si imposta alcuna password tutti i client possono accedere a smpppd.

slp-register = <yes | no> Il servizio di smpppd può essere reso noto sulla rete tramite SLP ricorrendo a questo parametro.

Per ulteriori informazioni su smpppd consultate le `man 8 smpppd` e `man 5 smpppd.conf`.

22.6.2 kinternet, cinternet e qinternet utilizzati da remoto

kinternet, cinternet e qinternet possono essere utilizzati per controllare un smpppd sia locale che remoto. cinternet è la variante testuale, che si basa sulla riga di comando, di kinternet che offre un' interfaccia grafica. qinternet e kinternet sono molto simili, si distinguono comunque per il fatto che qinternet non utilizza le librerie KDE, quindi potete installare qinternet a parte e utilizzarlo senza aver bisogno di KDE. Se volete utilizzare queste utility assieme ad uno smpppd remoto, dovrete editare il file di configurazione `/etc/smpppd-c.conf` manualmente o tramite kinternet. Questo file conosce solo tre opzioni:

sites = <elenco siti> Qui indicate ai front-end dove trovare smpppd. I front-end passeranno a setaccio le opzioni qui indicate nella sequenza riportata. L'opzione `local` indica la creazione della connessione al smpppd locale, `gateway` punta ad un smpppd sul gateway. La connessione va creata nel modo specificato sotto `server` nel file `config-file`. `slp` dà ai front-end l'istruzione di connettersi agli smpppd rilevati tramite SLP.

server = <server> Qui potete specificare l'host su cui gira smpppd.

password = <password> Immettete qui la password valida anche per smpppd.

Se smpppd è in esecuzione potete provare ad accedervi, ad esempio si consiglia di utilizzare in questi casi il comando `cinternet --verbose --interface-list`. Per maggiori dettagli consultate le pagine di manuale `man 5 smpppd-c.conf` e `man 8 cinternet`.

Servizi SLP sulla rete

Il *Service Location Protocol* (abbr. con SLP) è stato ideato per semplificare la configurazione di host collegati in rete all'interno di una rete locale. Per poter impostare un client di rete con tutti i servizi richiesti, l'amministratore deve disporre di informazioni dettagliate sui server presenti sulla rete. SLP indica la disponibilità di un determinato servizio a tutti i client di una rete locale. Applicazioni che supportano SLP si lasciano configurare in automatico grazie alle informazioni messe a disposizione da SLP.

SUSE LINUX supporta l'installazione tramite origini di installazione rilevate tramite SLP ed offre una serie di servizi di sistema con supporto integrato per SLP. YaST e Konqueror dispongono entrambi di front-end adatti a SLP. SLP su SUSE LINUX vi permette di mettere a disposizione dei vostri client collegati in rete funzionalità di primo piano come server di installazione, server YOU, server di file oppure di stampa.

23.1 Registrare servizi personalizzati

Numerose applicazioni sotto SUSE LINUX supportano già SLP grazie alla libreria `libslp`. Se volete rendere disponibili ulteriori servizi tramite SLP avete vari modi per realizzare il vostro intento:

Registrazione statica tramite `/etc/slp.reg.d`
Create per ogni servizio aggiuntivo un proprio file di registrazione. Riportiamo un esempio di un file del genere per la registrazione di un servizio riferito ad uno scanner:

```
## 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
```

Il rigo di maggior importanza di questo file è rappresentato dalla cosiddetta *service URL* che viene introdotta da `service:` indicante il tipo di servizio (`scanner.sane`) e l'indirizzo sotto il quale il servizio è disponibile sul server. ⟨*$HOSTNAME*⟩ viene sostituito automaticamente dal nome di host completo. Dopo i due punti segue la porta TCP sulla quale il servizio in questione è in ascolto. Immettete, separata da virgole, ancora la lingua nella quale il servizio debba presentarsi e la durata della registrazione espressa in secondi. Stabilite un valore per tale entità scegliendo un valore compreso nell'intervallo tra `0` e `65535`. Con `0` si impedisce la registrazione e con `65535` si elimina ogni restrizione.

Il file di registrazione contiene inoltre le variabili `watch-tcp-port` e `description`. La prima annuncia il servizio SLP solo se il rispettivo

servizio è abilitato, a tal fine slpd verifica lo stato del servizio. La seconda variabile contiene una precisa descrizione del servizio che viene visualizzata con browser adatti.

Registrazione statica tramite `/etc/slp.reg`
La sola differenza rispetto al procedimento descritto sopra è dovuta al fatto che tutti i servizi sono raggruppati in un file centrale.

Registrazione dinamica tramite slptool
Se la registrazione SLP di un servizio debba avvenire tramite propri script, utilizzate il front-end a linea di comando slptool.

23.2 Front-end SLP in SUSE LINUX

SUSE LINUX include diversi front-end che permettono di richiedere ed utilizzare informazioni SLP tramite rete:

slptool slptool è un programma da linea di comando semplice da utilizzare per l'invio di richieste SLP sulla rete oppure per indicare la disponibilità di determinati servizi. `slptool --help` elenca tutte le opzioni e funzionalità disponibili. Potete invocare slptool anche tramite degli script che elaborano dati SLP.

Browser SLP di YaST YaST offre sotto 'Servizi di rete' → 'Browser SLP' un proprio browser SLP che elenca in una struttura grafica ad albero tutti i servizi di una rete locale che sono stati resi noti tramite SLP.

Konqueror In veste di browser di rete Konqueror visualizza tutti i servizi SLP disponibili sulla rete locale se immettete `slp:/`. Cliccando sulle icone visualizzate nella finestra principale ottenete delle informazioni più dettagliate sul servizio selezionato.

Invocando in Konqueror invece `service:/` si può creare una connessione al servizio selezionato cliccando semplicemente sull' icona visualizzata nella finestra del browser.

23.3 Abilitare SLP

Se intendete mettere a disposizione dei servizi dovete lanciare slpd. Per richiedere solamente i servizi disponibili non è necessario lanciare il demone.

slpd viene lanciato, come la maggior parte dei servizi di sistema sotto SUSE LINUX tramite un proprio script di inizializzazione. Di default il demone non è attivo. Se volete attivarlo per la durata di una sessione, date come `root` il comando `rcslpd start` per lanciarlo e `rcslpd stop` per fermarlo. Tramite `restart` eseguite un riavvio e tramite `status` vi fate indicare lo stato attuale del demone. Se volete attivare slpd di default, date come `root` una sola volta il comando `insserv slpd`, in tal modo slpd verrà avviato automaticamente al boot del sistema.

23.4 Ulteriori informazioni

Per degli approfondimenti in tema di SLP consultate le seguenti fonti:

RFC 2608, 2609, 2610 L'RFC 2608 tratta in generale la definizione di SLP. L'RFC 2609 verte sulla sintassi delle url dei servizi utilizzate e RFC 2610 tratta DHCP via SLP.

http://www.openslp.com La home page del progetto OpenSLP.

file:/usr/share/doc/packages/openslp/* In questa directory trovate una raccolta esaustiva della documentazione su SLP incluso un `README.SuSE` contenente le specificazioni, gli RFC summenzionati e due documenti HTML introduttivi. Gli sviluppatori tra di voi che intendono utilizzare le funzionalità di SLP dovrebbero installare il pacchetto `openslp-devel` per poter utilizzare la *Programmers Guide* fornita a corredo.

24

DNS: Domain Name System

Compito del DNS Domain Name System è di risolvere i nomi di dominio e host in indirizzi IP. In tal modo l'indirizzo IP 192.168.0.1 viene assegnato ad esempio all'host `terra`. Prima di configurare un proprio server dei nomi, leggete le informazioni generali riguardanti il DNS che trovate nella sezione 22.3 a pagina 414. L'esempio di configurazione riportato si riferische a BIND

24.1 Configurazione con YaST

Il modulo DNS di vi consente di configurare un server DNS proprio nella rete locale. Questo modulo funziona in due modi. Al primo avvio del modulo l'amministratore deve prendere delle decisioni fondamentali. Una volta portata a termine la configurazione iniziale il server è preconfigurato e pronto ad essere impiegato. Il modo per esperti consente di eseguire interventi configurativi più complessi.

24.1.1 Configurazione guidata (Wizard)

Il wizard si compone di tre parti, che vi permettono di passare nel modo di configurazione per esperti.

Installazione del server DNS: impostazioni forwarder
Al primo avvio del modulo si avrà questa finestra (si veda la figura 24.1 a fronte. Stabilite se volete il demone PPP debba fornire un elenco di forwarder durante il processo di composizione tramite DSL o ISDN ('PPP Daemon stabilisce i forwarder') o se preferite di eseguire l'immissione voi stessi ('Stabilire forwarder manualmente').

Installazione del server DNS: zone DNS
Le registrazioni di questo modulo vengono spiegate nel modo di installazione da esperti (si veda la sezione 24.4 a pagina 459). Per una nuova zona va impostato un nome in 'Nome zona'. Per aggiungere una zona inversa, il nome deve terminare in `.in-addr.arpa`. Selezionate infine il 'Tipo di zona' (master o slave). Si veda la figura 24.2 a pagina 448. Cliccate su 'Modifica zona' per configurare altre impostazioni di una data zona. Per cancellare una zona cliccate su 'Elimina zona'.

Installazione del server DNS: chiudere il wizard
Visto che durante l'installazione viene abilitato un firewall, potete aprire la porta DNS nel firewall (Porta `53`) con 'Apri porta nel firewall' impostare il comportamento di avviamento del server DNS ('On' o 'Off'). Si veda la figura 24.3 a pagina 449.

24.1.2 Configurazione da esperti

Al primo avvio del modulo, visualizza una finestra con diverse possibilità di configurazione. In seguito, il server DNS è in linea di massima pronto ad essere utilizzato:

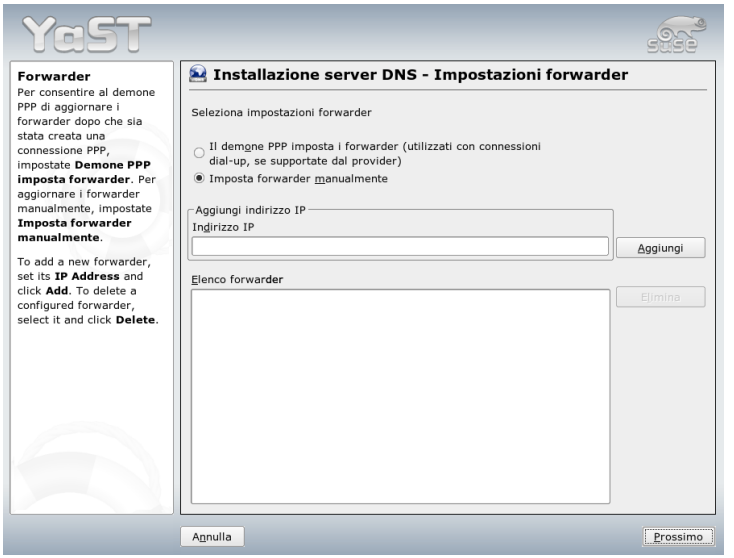

Figura 24.1: *Installazione del server DNS: forwarder*

Server DNS: avvio Sotto 'Avvio del sistema' potete accendere ('On') o spegnere il server DNS ('Off'). Tramite il bottone 'Avviare il server DNS ora' potete avviare il server DNS e fermarlo tramite 'Fermare server DNS ora'; salvare le impostazioni attuali vi è 'Salva impostazioni e riavvia il server DNS ora'.

Potete anche aprire la porta DNS ('Apri porta nel firewall') e tramite 'Dettagli firewall' intervenire in modo mirato sulle impostazioni del firewall.

Server DNS: forwarder Questa finestra è identica a quella che ottenete all'avvio del configurazione guidata wizard (si veda a fronte).

Server DNS: file di protocollo Qui stabilite cosa e dove il server DNS debba protocollare.

Sotto 'Tipo di protocollo' specificate dove il server DNS debba protocollare i suoi messaggi. Potete lasciare mano libera al sistema ('Protocollare nel protocollo di sistema' in `/var/log/messages`) oppure indicare esplicitamente un file ('Protocollare nel file'). In quest'ultimo caso, potete indicare

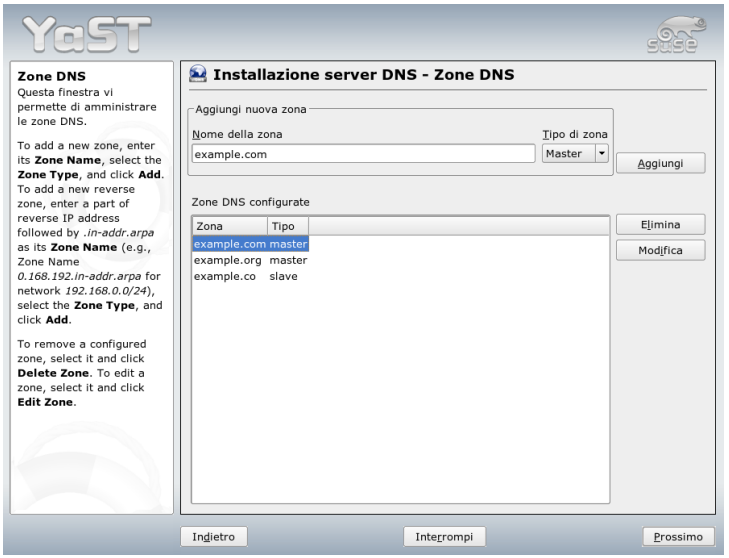

Figura 24.2: *Installazione del server DNS: zone DNS*

anche la dimensione massima del file in megabyte ed il numero dei file di protocollo.

Sotto 'Protocollare in aggiunta' potete impostare ulteriori opzioni: con 'Protocollare richieste' verrà protocollate *ogni* richiesta. Il file di protocollo raggiungere una notevole dimensione. Questa opzione si dovrebbe abilitare solo per eseguire il debug. Per eseguire un aggiornamento delle zone sul server DHCP e server DNS, selezionate 'Protocollare aggiornamento delle zone'. Per protocollare il traffico di dati durante il transfer dei dati zone (transfer delle zone) dal master allo slave abilitate l'opzione 'Protocollare transfer di zone' (si veda la figura 24.4 a pagina 450).

Server DNS: zone DNS Questa sezione è suddivisa in diverse finestre e tramite essa vengono amministrati i file zona (si veda la sezione 24.1.1 a pagina 446.

Server DNS: editor delle zone slave Arrivate a questa finestra se sotto in questa pagina avete selezionato 'Slave' come tipo zona. Sotto 'Server DNS master' indicate il server master a cui debba rivolgersi lo slave. Se intendete restrin-

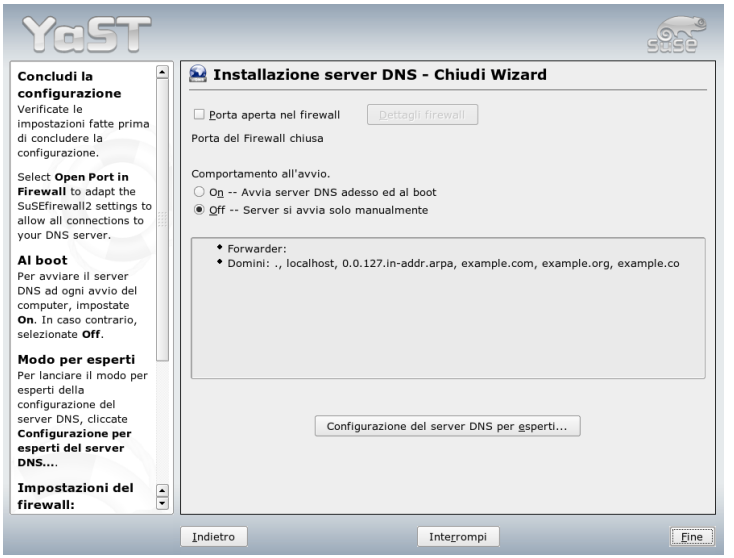

Figura 24.3: *Installazione del server DNS: chiudere il wizard*

gere l'accesso, potete selezionare le ACL definite in precedenza dall'elenco (si veda la figura 24.5 a pagina 451).

Server DNS: editor delle zone master
Arrivate a questa finestra se sotto nella pagina precedente avete selezionato come tipo di zona 'Master'. Potete visualizzare: Le 'basi'(la pagina attualmente visualizzata),'Registrazioni NS', 'Registrazioni MX', 'SOA' e 'Registrazioni'. Segue una breve illustrazione.

Server DNS: editor delle zone (registrazioni NS)
Qui potete stabilire dei server dei nomi alternativi per queste zone. Dovete badare al fatto che il proprio server dei nomi sia contenuto nell'elenco. Per aggiungere una nuova registrazione, indicate sotto 'Server dei nomi da aggiungere' il rispettivo nome e confermate con 'Aggiungi' (si veda la figura 24.6 a pagina 452).

Server DNS: editor delle zone (registrazioni MX)
Per aggiungere un nuovo server di posta per la zona attuale all'elenco es-

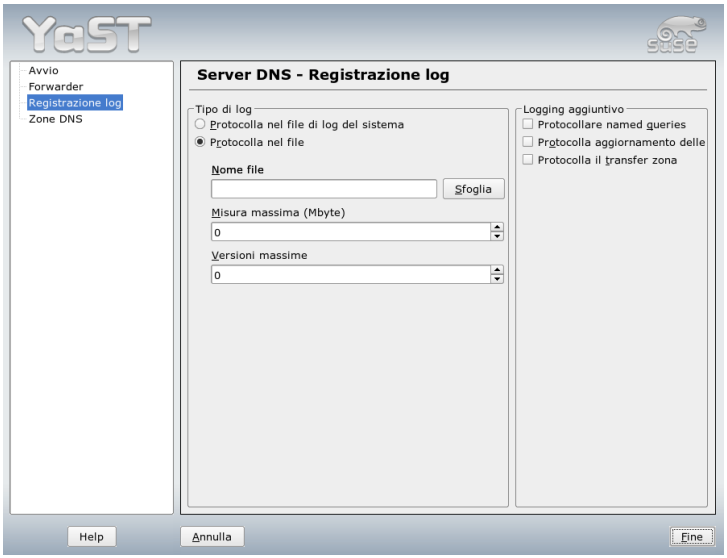

Figura 24.4: *Server DNS: attività di log*

istente, indicate il rispettivo indirizzo e la priorità. Confermate con 'Aggiungi' (si veda la figura 24.7 a pagina 453).

Server DNS: editor delle zone (SOA) Tramite SOA Record Configuration (si veda la figura 24.8 a pagina 454) si generano registrazioni SOA (*Start of Authority*). Il significato delle singole opzioni può essere evinto dall'esempio 24.6 a pagina 460. Ricordate che questa opzione non è disponibile nel caso di zone dinamiche amministrate da LDAP.

Server DNS: editor delle zone (Registrazioni)
Questa finestra amministra un elenco di coppie nomi e indirizzi IP. Nel campo di immissione sotto 'Chiave della registrazione' inserite il nome dell'host e selezionate il tipo (menu a tendina omonimo). 'A-Record' è la registrazione principale; 'CNAME' è un alias. Usate i tipi 'NS' e 'MX' per registrazioni dettagliati o parziali che si basano sulle informazioni fornite in 'Recordi NS' e 'Record MX'. Vi sono tra modi di risolvere una record A esistente. 'PTR' per le zone inverse è il contrario di una record A.

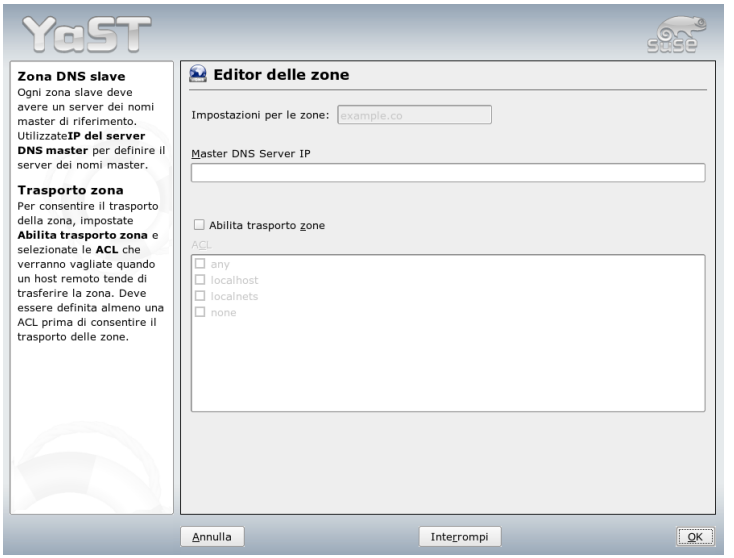

Figura 24.5: *Server DNS: editor delle zone slave*

24.2 Inizializzare il server dei nomi BIND

In SUSE LINUX, il server dei nomi BIND (*Berkeley Internet Name Domain*) è già preconfigurato in modo da poter essere avviato subito dopo l'installazione. Se siete già collegati ad Internet ed immettete in `/etc/resolv.conf` l'indirizzo `127.0.0.1` come server dei nomi per `localhost` avrete solitamente già una risoluzione dei nomi correttamente funzionante, senza dover conoscere il DNS del provider. BIND eseguirà la risoluzione dei nomi tramite i server dei nomi root – cosa che però richiede un pò di tempo. Per ottenere una risoluzione del nome sicura ed effettiva, immettete nel file di configurazione `/etc/named.conf`, sotto `forwarders`, il DNS del provider con indirizzo IP. Se tutto è andato per il verso giusto, il server dei nomi girerà nella modalità "caching-only". Solo dopo l'impostazione delle zone diventa un DNS a tutti gli effetti. Un esempio a riguardo è reperibile nella directory di documentazione `/usr/share/doc/packages/bind/sample-config`.

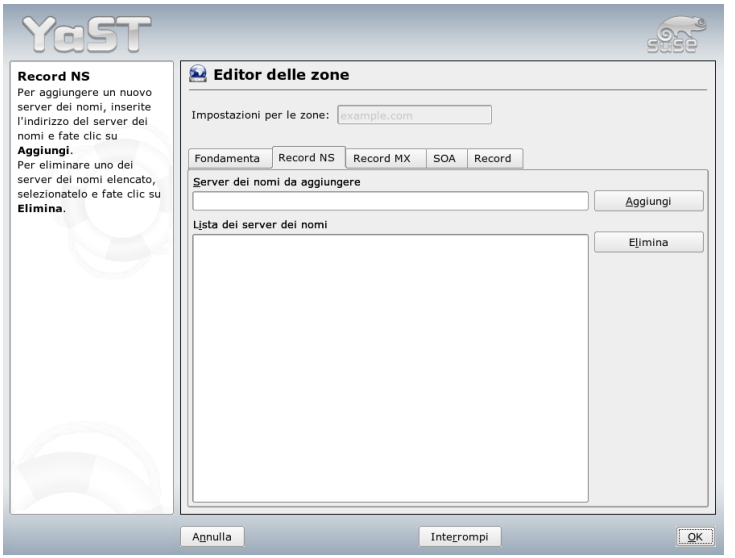

Figura 24.6: *Server DNS: editor delle zone (registrazioni NS)*

Suggerimento

Adattamenti automatici dell'allocazione dei nomi

A secondo del tipo di accesso ad Internet o ambiente di rete dato, l'allocazione dei nomi può essere adatta alla situazione attuale. A tal fine impostate la variabile `MODIFY_NAMED_CONF_DYNAMICALLY` nel file `/etc/sysconfig/network/config` su `yes`.

Suggerimento

Non si dovrebbe impostare un dominio ufficiale, finché l'autorità competente – per `.it` si tratta dell' ITNIC non ve ne assegni uno. Anche se avete un dominio personale, amministrato da un provider, non conviene utilizzarlo, dato che BIND non inoltrerebbe richieste indirizzate a questo dominio, e il server web del provider risulterebbe irraggiungibile per il proprio dominio.

Per avviare il server dei nomi, si immette come `root` di comando `rcnamed start`. Se sulla destra appare in verde "done", `named`, così si chiama il processo del server dei nomi, è stato inizializzato correttamente. Sul sistema

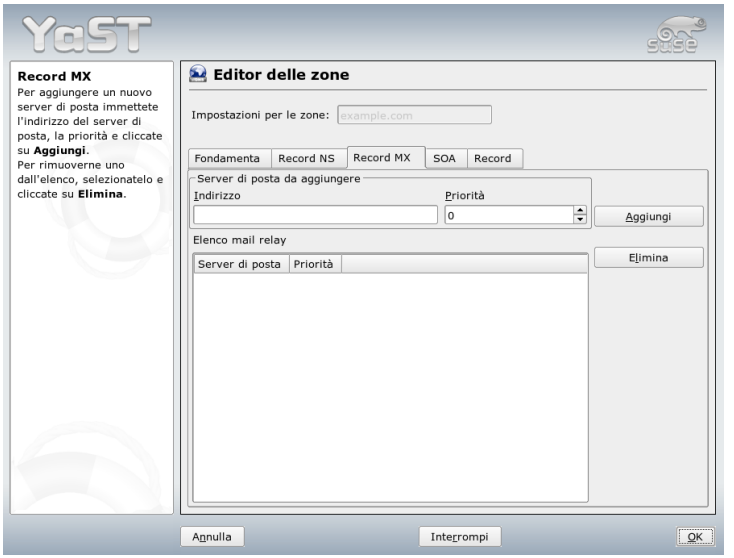

Figura 24.7: *Server DNS: editor delle zone (registrazioni MX)*

locale si potrà subito verificare se il server dei nomi funziona nel modo dovuto tramite i programmi `host` oppure `dig`. Come server di default deve venire indicato `localhost` con l'indirizzo `127.0.0.1`. Altrimenti in `/etc/resolv.conf` si trova probabilmente un server dei nomi sbagliato, o questo file non esiste. Per un primo test, inserite `host 127.0.0.1`; questo dovrebbe funzionare in ogni caso. Se invece ricevete una comunicazione di errore, controllate, con il seguente comando, se il `named` è in esecuzione con `rcnamed status`. Se il server dei nomi non parte o mostra qualche disfunzione, il motivo viene protocollato nella maggioranza dei casi sotto `/var/log/messages`.

Per usare come "forwarder" il server dei nomi del provider oppure un server dei nomi che gira all'interno della propria rete, bisogna registrarlo o registrarli nella sezione `options` sotto `forwarders`. Gli indirizzi IP utilizzati nel file esempio 24.1 nella pagina seguente sono stati scelti a caso, dovrete adattarli in base ai vostri dati effettivi.

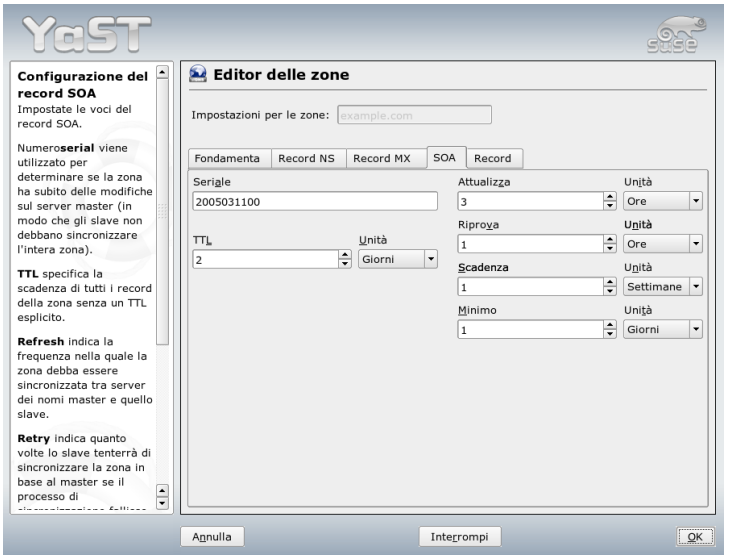

Figura 24.8: *Server DNS: editor delle zone (SOA)*

Esempio 24.1: *Opzioni di forwarding in 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;
        };
```

Dopo `options`, seguono le registrazioni per le zone, `localhost`, `0.0.127.in-addr.arpa` e il "." di "type hint" che dovrebbero essere presenti in ogni caso. I file corrispondenti non dovranno essere modificati, dal momento che funzionano benissimo così come sono. Non dimenticate di porre un ";" alla fine di ogni riga e di digitare correttamente le parentesi graffe. Dopo aver apportato delle modifiche al file di configurazione `/etc/named.conf` o ai file zona, BIND dovrà rileggerle, immettete dunque il comando `rcnamed reload`. Alternativamente, riavviate il server dei nomi con il comando `rcnamed restart`. E per terminare il server dei nomi, usate `rcnamed stop`.

24.3 Il file di configurazione /etc/named.conf

Tutte le impostazioni riguardanti il server dei nomi BIND devono venire eseguite nel file `/etc/named.conf`. Anche i dati delle zone, cioè i nomi degli host, gli indirizzi IP, etc. per i domini da amministrare, devono venire archiviati in file separati nella directory `/var/lib/named`. Trattateremo questo tema più avanti.

L' `/etc/named.conf` si suddivide grosso modo in due settori: una sezione `options` per le impostazioni generali ed una per le registrazioni `zone` per i singoli domini. Inoltre è anche possibile definire un'area `logging`, come pure registrazioni del tipo `acl` (ingl.Access Control List). Le righe di commento iniziano con il carattere #, alternativamente è permesso anche `//`. Il file esempio 24.2 in questa pagina vi mostra un esempio di un `/etc/named.conf` minimale.

Esempio 24.2: *File /etc/named.conf di base*

```
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 Le opzioni di configurazione principali

directory "⟨*nomefile*⟩"; indica la directory in cui BIND trova i file con i dati delle zone, di solito `/var/lib/named`.

forwarders { ⟨*indirizzo ip*⟩; }; viene usato per indicare uno o più server dei nomi (nella maggioranza dei casi quelli del provider) ai quali vengono inoltrate le richieste DNS a cui non è possibile rispondere direttamente. Al posto di ⟨*indirizzo ip*⟩ utilizzato un indirizzo IP del tipo `10.0.0.1`.

forward first; fa in modo che le richieste DNS vengano inoltrate `forwarded`, prima che si cercare di risolverle tramite i server dei nomi root. Invece di `forward first` è anche possibile scrivere `forward only`; in questo caso, tutte le richieste vengono inoltrate ed i server dei nomi root non vengono più indirizzati. Può essere conveniente in configurazioni firewall.

listen-on port 53 {127.0.0.1; ⟨*indirizzo ip*⟩; };
comunica a BIND, su quali interfacce di rete e su quale porta mettersi in ascolto di eventuali richieste dei client. L'indicazione `port 53` può venire omessa, poiché `53` è la porta standard. Con `127.0.0.1` si ammettono richieste di localhost. Omettendo completamente questa registrazione, vengono usate di default tutte le interfacce.

listen-on-v6 port 53 { any; }; indica a BIND su quale porta mettersi in ascolto di richieste da parte di client che utilizzano IPv6. Oltre a `any` è consentito come alternativa solo `none`, dato che il server si mette in ascolto sull'indirizzo wildcard IPv6.

query-source address * port 53; questa registrazione è necessaria se il firewall blocca richieste DNS esterne. In questo modo BIND viene indotto ad inviare delle richieste verso l'esterno dalla porta 53 e non dalle porte con un numero elevato (> 1024).

query-source-v6 address * port 53; qui si indica a BIND quale porta utilizzare per richieste IPv6.

allow-query {127.0.0.1; ⟨*net*⟩; }; definisce le reti da cui i client possono inviare delle richieste DNS. Al posto di ⟨*net*⟩ si immettete un indirizzo del tipo `192.168.1/24`; laddove `/24` è un'abbreviazione per la maschera di rete, in questo caso `255.255.255.0`.

allow-transfer {! *; }; regola quali sistemi possano richiedere il trasferimento delle zone; in questo esempio ciò viene completamente impedito da `! *`.

Senza questa registrazione, il trasferimento delle zone può venire richiesto da ovunque.

statistics-interval 0; senza questa registrazione, BIND archivia ogni ora diverse righe di messaggi di natura statistica in `/var/log/messages`. Il valore 0 determina che questi messaggi vengano completamente soppressi; l'intervallo viene indicato in minuti.

cleaning-interval 720; questa opzione stabilisce l'intervallo di tempo, scaduto il quale BIND svuota la sua cache. Ogni volta questa attività genera una registrazione in `/var/log/messages`. L'indicazione del tempo avviene in minuti: sono preconfigurati 60 minuti.

interface-interval 0; BIND verifica regolarmente se vi sono delle nuove interfacce di rete o se ne sono state rimosse alcune. Se questo valore è impostato su `0`, si rinuncia a tale verifica, e BIND si mette in ascolto solo sulle interfacce rilevate all'avvio. Si può indicare questo l'intervallo in minuti. 60 minuti è il valore preconfigurato.

notify no; Con `no` non viene avvisato nessun altro server dei nomi nel caso si siano apportate delle modifiche ai dati delle zone o se il server dei nomi viene riavviato.

24.3.2 Attività di logging

BIND permette di configurare in modo flessibile l'attività di logging. Normalmente, le preimpostazioni dovrebbero rilevarsi sufficienti. Il file esempio 24.3 in questa pagina vi mostra la variante più semplice di una tale registrazione, e sopprime completamente il "logging":

Esempio 24.3: *Il logging viene soppresso*

```
logging {
        category default { null; };
};
```

24.3.3 Struttura delle registrazioni delle zone

Esempio 24.4: *L'indicazione zone per mio-dominio.it*

```
zone "mio-dominio.it" in {
       type master;
       file "mio-dominio.zone";
       notify no;
};
```

Dopo `zone` si indica il nome del dominio da amministrare, nel nostro esempio abbiamo scelto un nome a caso `mio-dominio.it` seguito da un `in` ed un blocco compreso tra parentesi graffe con le relative opzioni; cfr. esempio 24.4 in questa pagina. Se si desidera definire una *zona slave*, cambia solo il `type` che diventa `slave`, e si deve indicare il server dei nomi che amministra questa zona come `master` (può, a sua volta essere uno "slave"); si veda l'esempio 24.5 in questa pagina.

Esempio 24.5: *L'indicazione zone per altro-dominio.it*

```
zone "altro-dominio.it" in {
        type slave;
        file "slave/altro-dominio.zone";
        masters { 10.0.0.1; };
};
```

Le opzioni di zone:

type master; `master` stabilisce che questa zona venga amministrata su questo server di nome. Premessa per questa opzione: un file di zone corretto.

type slave; Questa zona viene trasferita da un altro server dei nomi. Deve venire usata assieme a `masters`.

type hint; La zona `.` del tipo `hint` viene impiegata per l'indicazione dei server dei nomi root. Questa definizione di zona può rimanere invariata.

file `mio-dominio.zone` o file "slave/altro-dominio.zone";
Questa registrazione indica il file in cui sono registrati i dati delle zone per il dominio. Con uno slave, il file non è necessario, poiché il suo contenuto viene preso da un altro server dei nomi. Per distinguere fra file master e file slave, si indica la directory `slave` per i file slave.

masters {⟨*indirizzo_ip_server*⟩; }; Questa impostazione è necessaria solo per zone slave ed indica da quale server dei nomi debba venire trasferito il file delle zone.

allow-update {! *; }; Questa opzione regola l'accesso in scrittura ai dati delle zone dall'esterno. Se l'accesso fosse indiscriminato, ogni client potrebbe registrarsi nel DNS del tutto autonomamente, cosa non auspicabile da un punto di vista della sicurezza. Senza questa opzione, non sono permessi gli aggiornamenti delle zone. La registrazione riportata nell'esempio non cambierebbe nulla, dal momento che la definizione `! *` proibisce, anch'essa, ogni accesso.

24.4 Struttura di un file zona

Servono due tipi di file zona: uno per attribuire un indirizzo IP al nome di un host e l'altro per fare l'esatto contrario, cioè allocare un nome host ad un determinato indirizzo IP.

Suggerimento

Il punto (.) nei file zona

D'importanza fondamentale è il `.` nei file zona. A nomi di host senza il punto finale viene sempre aggiunta automaticamente la zona. E' quindi necessario porre un `.` alla fine di nomi completi, già provvisti di dominio completo, per evitare che il dominio venga aggiunto una seconda volta. La mancanza di questo punto alla fine o la sua posizione errata sono sicuramente gli errori più comuni nella configurazione di server dei nomi.

Suggerimento

Osserviamo ora il file zona `mondo.zone` responsabile per il dominio Domain `mondo.all` mostrato nell'esempio 24.6 nella pagina successiva.

Esempio 24.6: *File /var/lib/named/mondo.zone*

```
$TTL 2D
mondo.all IN SOA      gateway  root.mondo.all.(
              2003072441  ; serial
              1D          ; refresh
              2H          ; retry
              1W          ; expiry
              2D )        ; minimum

             IN NS       gateway
             IN MX       10 sole

 gateway     IN A        192.168.0.1
             IN A        192.168.1.1
 sole        IN A        192.168.0.2
 luna        IN A        192.168.0.3
 terra       IN A        192.168.1.2
 marte       IN A        192.168.1.3
 www         IN CNAME    luna
```

Rigo 1: `$TTL` definisce il TTL standard (ingl. Time To Live), ovvero la scandenza valida per l'intero contenuto di questo file: due giorni, in questo caso `2D`= 2 days)..

Rigo 2: Ha inizio qui il `SOA control record` (SOA = Start of Authority):

- Al primo posto vi è il nome del dominio da amministrare `mondo.all`, con un `.` alla fine, per evitare che venga aggiunta la zona una seconda volta. Alternativamente, si può digitare una chiocciola `@`, in questo caso la zona viene evinta dalla rispettiva registrazione in `/etc/named.conf`.
- Dopo l'`IN SOA`, abbiamo il nome del server dei nomi, responsabile per questa zona in funzione di master. In questo caso, il nome `gateway`, diventa automaticamente `gateway.mondo.all`, perché non seguito da un `.`.
- Segue l'indirizzo e-mail della persona responsabile per il server dei nomi. Dal momento che la chiocciola `@` possiede già un significato particolare, si aggiungerà semplicemente un `.`, di modo che, al posto di `root@mondo.all` avremo `root.mondo.all.`; non dimenticate il punto alla fine, altrimenti viene aggiunta la zona una seconda volta.

- Alla fine abbiamo una `(`, per includere i righi seguenti fino alla seconda `)` nella istruzione SOA.

Rigo 3: Il `numero di serie` è una cifra arbitraria, da aumentare ogni volta che si modifica questo file. Questa cifra serve ad informare server dei nomi secondari (server slave) che sono state effettuate delle modifiche. Di solito, si usa un numero di dieci cifre composto da una data e da un numero progressivo, nella forma `AAAAMMGGNN`.

Rigo 4: Il `refresh rate` indica l'intervallo di tempo trascorso il quale i server dei nomi secondari verificano il `numero di serie` della zona. In questo caso, si ha 1 giorno (1D = 1 day).

Rigo 5: Il `retry rate` indica l'intervallo di tempo trascorso il quale un name server secondario, in caso di errore, cerca di ristabilire il contatto con il server primario. In questo caso, due ore (2H = 2 hours).

Rigo 6: L'`expiration time` indica quanto tempo debba passare prima che il server dei nomi secondario espelli i dati dalla cache, se non riesce a ristabilire il contatto con il server primario. In questo caso, una settimana (1W = 1 week).

Rigo 7: Con `negative caching TTL` si conclude l'SOA, che indica per quanto tempo i risultati delle richieste DNS di altri server irrisolte debbano restare nella cache.

Rigo 9: L'`IN NS` indica il server dei nomi responsabile per questo dominio. Anche in questo caso, `gateway` diventa automaticamente `gateway.mondo.all`, poiché non vi è un `.` alla fine. Vi possono essere diverse righe del genere: una per il server dei nomi primario e una per ogni server dei nomi secondario. Se per questa zona `notify` in `/etc/named.conf` non è impostato su `no`, verranno informati tutti i server dei nomi qui elencati delle modifiche apportate ai dati delle zone.

Rigo 10: La registrazione MX indica il server di posta che accetta le e-mail per il dominio `mondo.all`, per poi elaborarle o inoltrarle. In quest'esempio, si tratta dell'host `sole.mondo.all`. Il numero davanti al server dei nomi è il valore di preferenza: se vi sono più indicazioni MX, si prenderà per primo il server di posta con il valore minore; se la consegna a questo server fallisce, si prova con il prossimo valore.

Righe 12-17: Le registrazioni degli indirizzi (ingl. Address Records), dove il nome dell'host viene attribuito ad uno o più indirizzi IP. In questo caso, i nomi vengono riportati senza un punto alla fine, dal momento che sono registrati senza il relativo dominio e che in questo caso è possibile aggiungere a tutti `mondo.all`. A `gateway` sono stati attribuiti due indirizzi IP, dacché dispone di due schede di rete. `A` sta per un indirizzo host tradizionale; con `A6` si immettono indirizzi IPv6 e `AAAA` è il formato ormai superato per indirizzi IPv6.

Rigo 18: Impostare un alias per `www`, p.es `luna` (`CNAME` = *canonical name* ovvero nome canonico).

Per la risoluzione inversa (ingl. reverse lookup) degli indirizzi IP in nomi di host si ricorre allo pseudo-dominio `in-addr.arpa` che viene aggiunto all'indirizzo scritto alla rovescia. Quindi, `192.168.1` diventa `1.168.192.in-addr.arpa`. Si veda l'esempio 24.7 in questa pagina.

Esempio 24.7: *Risoluzione inversa dell'indirizzo*

```
1
2  $TTL 2D
3  1.168.192.in-addr.arpa. IN SOA gateway.mondo.all. root.mondo.all. (
4                           2003072441     ; serial
5                           1D              ; refresh
6                           2H              ; retry
7                           1W              ; expiry
8                           2D )            ; minimum
9
10                          IN NS           gateway.mondo.all.
11
12 1                     IN PTR          gateway.mondo.all.
13 2                     IN PTR          terra.mondo.all.
14 3                     IN PTR          marte.mondo.all.
```

Rigo 1: $TTL definisce il TTL di default valido per tutte le voci.

Rigo 2: Questo file permette il "reverse lookup" per la rete `192.168.1.0`. Dal momento che la zona del caso è `1.168.192.in-addr.arpa`, non la si vorrà aggiungere al nome del server: per questo motivo, i nomi sono tutti completi di dominio e punto finale. Il resto corrisponde all'esempio dato per `mondo.all`.

Righe 3-7: si veda l'esempio di `mondo.all`.

Rigo 9: Questa riga indica nuovamente il server dei nomi responsabile per questa zona. Questa volta, però, il nome viene riportato completo di dominio e punto finale.

Righe 11-13: Le registrazioni pointer (puntatore) puntano sull' indirizzo IP del relativo host. All'inizio della riga trovate solo la parte finale dell'indirizzo, senza `.` finale. Se ora aggiungete la zona e togliete `.in-addr.arpa`, avrete l'indirizzo IP completo, scritto alla rovescia.

Il trasferimento di zone tra le diverse versioni di BIND di solito non dovrebbe creare dei problemi.

24.5 Aggiornamento dinamico dei dati di zona

Con aggiornamento dinamico (ingl. dynamic update) si intende l'aggiunta, la modifica e l'eliminazione di registrazioni nei dati zona di un master. Questo meccanismo viene descritto nell'RFC 2136. L'aggiornamento dinamico delle zone si configura tramite le opzioni `allow-update` o `update-policy` nelle registrazioni delle zone. Le zone che vengono aggiornate dinamicamente non dovrebbero venir impostate manualmente.

Con `nsupdate` le registrazioni da aggiornare vengono trasmesse al server; per la corretta sintassi si veda la pagina di manuale di nsupdate (`man 8 nsupdate`). L'aggiornamento deve avvenire assolutamente, per motivi di sicurezza, tramite transazioni sicure (TSIG); cfr. la sezione 24.6 in questa pagina.

24.6 Transazioni sicure

Grazie alle "Transaction SIGnatures" (TSIG) si realizza una transazione sicura. Vengono utilizzate delle chiavi di transazione (ingl. transaction keys) e firme di transazione (ingl. transaction signatures). Nella seguente sezione spiegheremo come generarle ed utilizzarle.

Una transazione sicura è richiesta per la comunicazione tra server e l'aggiornamento dinamico dei dati di zona. Il controllo degli accessi basato su chiave offre maggior sicurezza rispetto ad un controllo basato sugli indirizzi IP.

Con il seguente comando potete generare una chiave di transazione (per avere ulteriori informazioni si veda la pagina di manuale `man dnssec-keygen`):

dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2

Il risultato sono due file che per esempio portano il seguente nome:

```
Khost1-host2.+157+34265.private
Khost1-host2.+157+34265.key
```

La chiave è contenuta in entrambi i file (p.es. `ejIkuCyyGJwwuN3xAteKgg==`). In seguito `Khost1-host2.+157+34265.key` dovrebbe venir copiato in modo sicuro (p.es. con `scp`) su host remoti e lì essere inserito in `/etc/named.conf` per realizzare una comunicazione sicura tra `host1` e `host2`:

```
?dbsuse-latex font-size="footnotesize" ?>
key host1-host2. {
  algorit        hm hmac-md5;
  secret "ejIkuCyyGJwwuN3xAteKgg=="
};
```

Avvertimento

Permessi di accesso di `/etc/named.conf`

Assicuratevi che i permessi di accesso per `/etc/named.conf` rimangono limitati; il valore di default è `0640` per `root` ed il gruppo `named`; alternativamente potete archiviare la chiave in un file protetto ed includerlo in seguito.

Avvertimento

Affinché sul server `host1` venga utilizzata la chiave per `host2` con l'indirizzo esempio `192.168.2.3` il file `/etc/named.conf` sul server deve contenere:

```
server 192.168.2.3 {
   keys { host1-host2. ;};
};
```

Il file di configurazione di `host2` deve essere adattato di conseguenza.

Oltre alle ACL che si basano sugli indirizzi IP e area degli indirizzi si dovrebbero aggiungere delle chiavi TSIG per avere delle transazioni sicure; ecco un esempio:

```
allow-update { key host1-host2. ;};
```

Per ulteriori informazioni consultate nel manuale di amministrazione di BIND (*BIND Administrator Reference Manual*) la parte intitolata `update-policy`.

24.7 DNSSEC

DNSSEC (DNS Security) viene illustrato nell'RFC 2535; gli strumenti disponibili per l'utilizzo di DNSSEC sono descritti nella manuale di BIND.

Una zona per dirsi sicura deve avere una o più chiavi zona; questo tipo di chiave viene generato - come nel caso di chiavi per host - con `dnssec-keygen`. Ai fini della cifratura al momento si usa DSA. Le chiavi pubbliche (public keys) dovrebbero essere integrate nei file zona con `$INCLUDE`.

Tutte le chiavi possono essere riunite in un set di chiavi tramite `dnssec-makekeyset` da trasmettere in modo sicuro alla zona superiore (parent zone), per essere firmati con `dnssec-signkey`. I file creati durante questo processo, vanno utilizzati ai fini della firma delle zone assieme a `dnssec-signzone` e i file generati da questo processo vanno quindi integrati in `/etc/named.conf` nella zona corrispondente.

24.8 Ulteriori informazioni

Rimandiamo al *BIND Administrator Reference Manual* che trovate sotto `/usr/share/doc/packages/bind/`; segnaliamo inoltre gli RFC ricordati enl manuale e le pagine di manuale di BIND. `/usr/share/doc/packages/bind/README.SuSE` offre delle informazioni aggiornate su BIND in SUSE LINUX.

NIS: Network Information Service

Non appena i sistemi Unix a voler accedere a risorse condivise sulla rete diventano più di uno, nasce l'esigenza di assicurare che non si verificano dei conflitti da ricondurre agli ID degli utenti e dei gruppi. La rete deve essere trasparente per gli utenti, in modo che, da qualsiasi computer l'utente lavori, egli si trovi di fronte sempre allo stesso ambiente. Questo viene reso possibile dai servizi NIS e NFS. L'NFS serve alla dislocazione di file system nella rete e viene descritto più dettagliatamente nel capitolo 26 a pagina 473.

NIS (ingl. Network Information Service) può essere visto come servizio di database che consente di accedere da ogni punto della rete alle informazioni dei file `/etc/passwd`, `/etc/shadow` oppure `/etc/group`. NIS può essere utilizzato anche per altri scopi (ad esempio per `/etc/hosts` oppure `/etc/services`). Comunque in questo capitolo non si approfondirà questo aspetto. Per NIS si utilizza spesso come sinonimo l'espressione *YP* che deriva da *yellow pages*, dunque *pagine gialle* nella rete.

25.1 Server slave e master NIS

Ai fini della configurazione selezionate in YaST 'Servizi di rete' e lì 'Server NIS'. Se nella vostra rete non vi è ancora un server NIS, nella prossima maschera dovete attivare la voce 'Installa e imposta server NIS master'. Se avete già un server NIS (dunque un "master"), potete aggiungere (ad esempio quando configurate una nuova sottorete) un server NIS slave. Iniziamo con la configurazione del server master. Se non sono installati tutti i pacchetti necessari vi chiederà di inserire il relativo CD o il DVD per poter eseguire l'installazione dei rispettivi pacchetti. Nella prima maschera di configurazione (si veda la figura 25.1 nella pagina successiva) immettete in alto il nome di dominio. Nella checkbox (nella parte inferiore) potete stabilire, se il computer debba anche fungere da client NIS, dunque se deve essere consentito agli utente di eseguire il login e ottenere poi i dati dal server NIS.

Se volete impostare un ulteriore server NIS ("Slave-Server") nella vostra rete, attivate la box 'Esiste un server NIS slave attivo'. Inoltre va attivata la voce 'Distribuzione map veloce' che comporta che le registrazioni del database vengano trasmessi quasi istantaneamente dal server master a quello slave.

Qui inoltre, potete, se volete, permettere agli utenti della vostra rete di modificare le loro password (con il comando `yppasswd`, dunque non solo localmente ma anche quelle deposte sul server NIS). In seguito sono attivate anche le caselle 'Permetti di cambiare il campo GECOS' e 'Permetti di cambiare la shell'. "GECOS" significa che l'utente può modificare le impostazioni riguardanti il suo nome ed indirizzo (con il commando `ypchfn`). "SHELL" vuol dire che l'utente può modificare anche la shell predefinita (tramite il comando `ypchsh`, ad es. da bash a sh).

Cliccando su 'Impostazioni globali...' giungete a una finestra di dialogo (si veda la figura 25.2 a pagina 470), in cui si può modificare la directory sorgente del server NIS (di default `/etc`). Inoltre qui si possono raggruppare password e

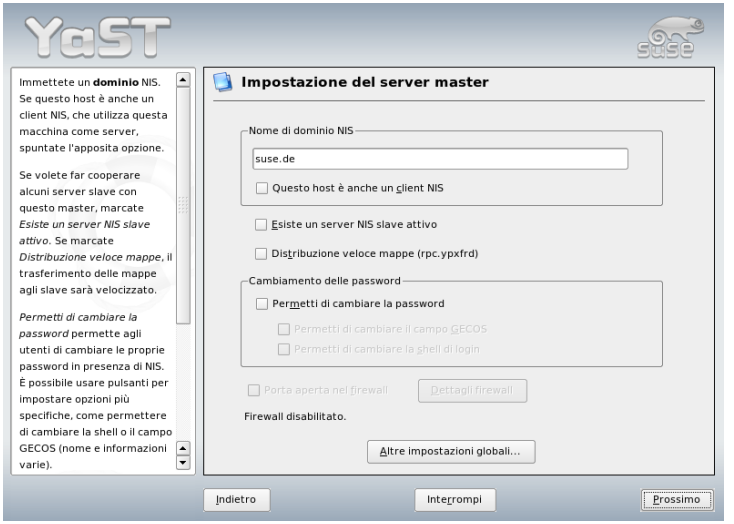

Figura 25.1: *: tool di configurazione per server NIS*

gruppi. L'impostazione dovrebbe essere lasciata su 'Sì' in modo che i rispettivi file (`/etc/passwd` e `/etc/shadow` o `/etc/group`) vengano allineati. Inoltre si può stabilire il numero di ID di utente e gruppi. Con 'OK' confermate le vostre immissioni e giungete nuovamente alla maschera precedente. Cliccate qui su 'Prossimo'.

Se avete già abilitato la voce 'Esiste un server NIS slave attivo', dovete immettere i nomi degli host che dovranno fungere da slave. Stabilite il nome e fate clic su 'Prossimo'. Se nella vostra rete non vi è nessun server slave giungete direttamente alla finestra di dialogo successiva per le impostazioni della banca dati. Qui potete impostare le "mappe", vale a dire banche dati parziali, che dal server NIS devono essere trasferite sui rispettivi client. Nella maggioranza dei casi si sconsiglia di modificare le preimpostazioni. Se intendete modificarle, fatelo solo con cognizione di causa.

Con 'Prossimo' arrivate all'ultima finestra di dialogo, dove potete stabilire da quali reti possono provenire richieste per il server NIS (si veda la figura 25.3 a pagina 471). Di solito si tratterà della vostra rete aziendale, in questo caso dovrebbero esserci le registrazioni

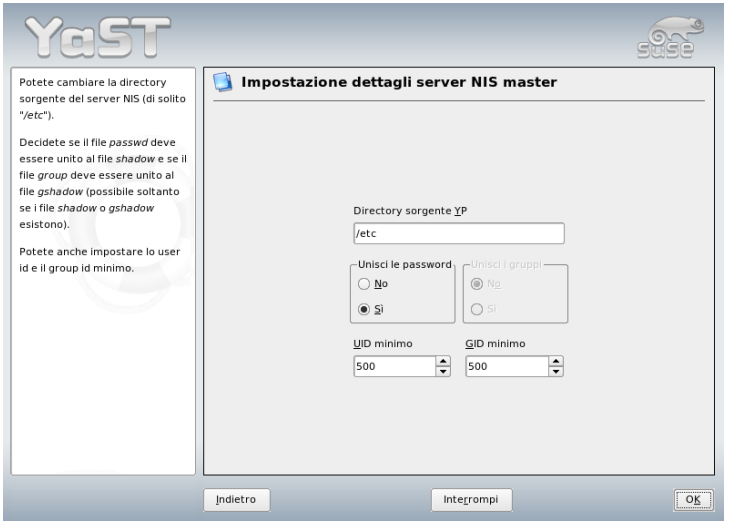

Figura 25.2: *: server NIS: modificare directory e sincronizzare file*

```
255.0.0.0 127.0.0.0
0.0.0.0   0.0.0.0
```

La prima permette connessioni dal proprio computer, e la seconda permette a tutti i computer con accesso alla rete di inviare delle richieste al server.

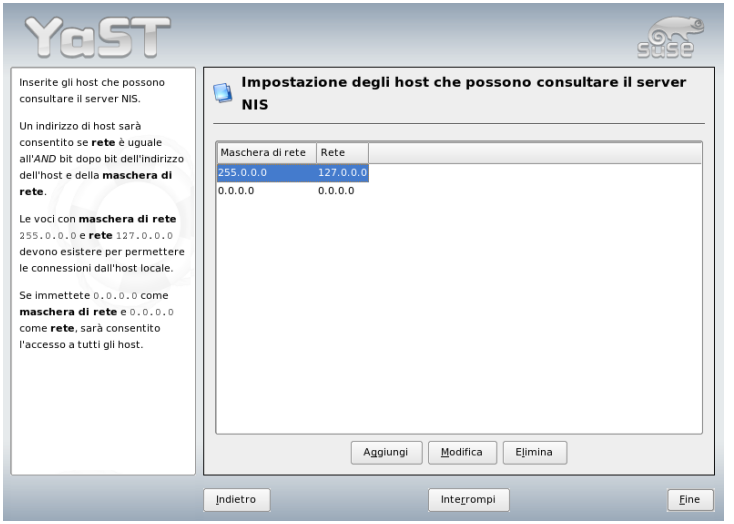

Figura 25.3: *Server NIS: gli host con permesso di inviare richieste*

Importante

Configurazione automatica del firewall

Se sul vostra sistema gira una firewall (SuSEfirewall2), YaST ne adatta la configurazione per il server NIS, non appena selezionate 'Porte aperte nel firewall'. YaST abiliterà quindi il servizio `portmap`.

Importante

25.2 Il modulo client NIS in YaST

Questo modulo YaST vi permette di configurare facilmente il client NIS. Dopo che nel dialogo iniziale avete indicato che intendete utilizzare NIS ed eventualmente l'automounter giungete alla finestra di dialogo successiva. Qui potete indicare se il client NIS dispone di un indirizzo IP statico oppure se riceverà l'indirizzo via DHCP, in questo caso non potete indicare un dominio NIS o indirizzo IP del server, poiché questi dati vengono assegnati tramite DHCP. Per ulteriori

informazioni su DHCP consultate la capitolo 27 a pagina 479. Se il client dispone di un indirizzo IP fisso, dovete immettere manualmente il dominio e server NIS (si veda la figura 25.4 in questa pagina). Tramite il pulsante 'Cerca', YaST cercherà un server NIS attivo nella rete.

Avete anche la possibilità di indicare domini multipli con un dominio di default. Per i singoli domini poi, con 'Aggiungi' potete indicare più server e la funzione broadcast.

Nelle impostazioni per esperti potete evitare che un host nella rete possa chiedere ad un'altro client quale sia il server utilizzato dal vostro client. Se abilitate 'Broken Server' verranno accettate anche delle risposte da un server su una porta non privileggiata. Per maggiori dettagli consultate la pagina di manuale di `ypbind`.

Figura 25.4: *Indicazione del dominio e dell'indirizzo del server NIS*

Condividere file system condivisi tramite NFS

Come abbiamo già accennato nella capitolo 25 a pagina 467, l'NFS e l'NIS rendono la rete trasparente per l'utente. L'NFS permette di dislocare i file system nella rete. Non importa su quale computer l'utente lavora, egli si troverà sempre di fronte allo stesso ambiente.

Sia l'NIS che l'NFS sono servizi asimmetrici. Vi è il server NFS ed il client NFS, ma ogni computer può fungere contemporaneamente sia da server che da client NFS, ovvero mettere a disposizione dei file system nella rete ("esportare"), e montare file system di altri host ("importare"). Normalmente, tuttavia, si usano a questo scopo dei server con dischi capienti, i cui file system vengono poi montati dai client.

Importante

DNS richiesto

In linea di massiama tutti gli export possono realizzarsi solo tramite indirizzi IP. Per evitare delle scadenze di tempo massimo si consiglia di lavorare con un sistema DNS. Ciò è necessario già per ragioni di logging, poiché il demone mountd esegue dei reverse lookup.

Importante

26.1 Importare file system con YaST

Ogni utente (che dispone dei relativi permessi), può montare directory NFS da un server NFS nel proprio albero di file. Il modo più semplice di farlo è quello di ricorrere al modulo 'Client NFS' di . Si deve solo immettere il nome host del computer che funge da server NFS, la directory da esportare e il punto di montaggio sul vostro computer. Nella prima finestra di dialogo selezionate 'Aggiungi' ed immettete le indicazioni sovramenzionate (si veda la figura 26.1 in questa pagina).

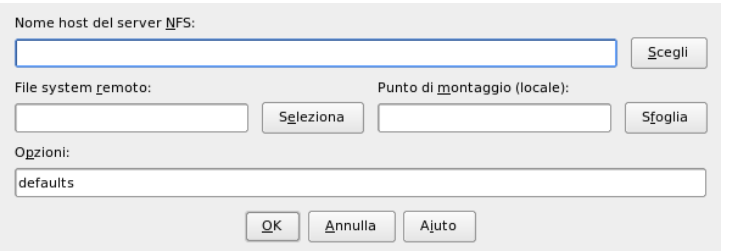

Figura 26.1: *Configurare il client NFS*

26.2 Importare manualmente i file system

Importare manualmente file system da un server NFS è molto facile. L' unico requisito è che sia stato avviato il portmapper RPC, avendo immesso il comando

`rcportmapstart` come utente `root`. Dopodiché sarà possibile includere file system estranei nel proprio file system (a condizione che essi siano stati esportati dai relativi computer) in modo analogo ai dischi locali, ovvero con il comando `mount`. La sintassi è la seguente:

```
mount host:percorso-remoto percorso-locale
```

Per importare, ad esempio, le directory degli utenti dall'host sole, usate il comando:

```
mountsole:/home /home
```

26.3 Esportare file system con YaST

YaST, vi permette di trasformare in poco tempo un computer della vostra rete in un server NFS: un server che mette a disposizione delle directory e dei file a tutti i computer con relativo permesso di accesso. Gli utenti possono usufruire e utilizzare così applicativi senza doverli installare localmente sul loro computer. Per eseguire l'installazione selezionate in YaST: 'Servizi di rete' → 'Server NFS'. (si veda la figura 26.2 nella pagina seguente).

Selezionate quindi 'Avvia server NFS' e fate clic su 'Prossimo'. Nella campo superiore immettete le directory da esportare, e in quella inferiore gli host della vostra rete con il permesso di accesso (si veda la figura 26.3 a pagina 477). Per ogni host possono essere settate quattro opzioni, `host singolo`, `gruppi di rete`, `wildcard` e `reti IP`. Per una descrizione dettagliata di queste opzioni provate con `man exports`. 'Esci' completa la configurazione.

Importante

Configurazione automatica del firewall

Se sul vostro sistema gira un firewall (SuSEfirewall2), YaST ne adatta la configurazione per il server NFS non appena selezionate 'Porte aperte nel firewall'. YaST abiliterà quindi il servizio `nfs`.

Importante

Figura 26.2: *Tool di configurazione per server NFS*

26.4 Esportare manualmente i file system

Se eseguite la configurazione manualmente senza ricorrere a YaST, dovete assicurare che sul server NFS vengano inizializzati i seguenti servizi:

- RPC portmapper (portmap)
- RPC mount daemon (rpc.mountd)
- RPC NFS daemon (rpc.nfsd)

Affinché al boot del sistema vengano avviati dagli script `/etc/init.d/portmap` ed `/etc/init.d/nfsserver` dovete immettere i comandi `insserv /etc/init.d/nfsserver` e `insserv /etc/init.d/portmap`. Inoltre, dovrà essere specificato quali file system debbano essere esportati su quali computer. Ciò avviene nel file `/etc/exports`.

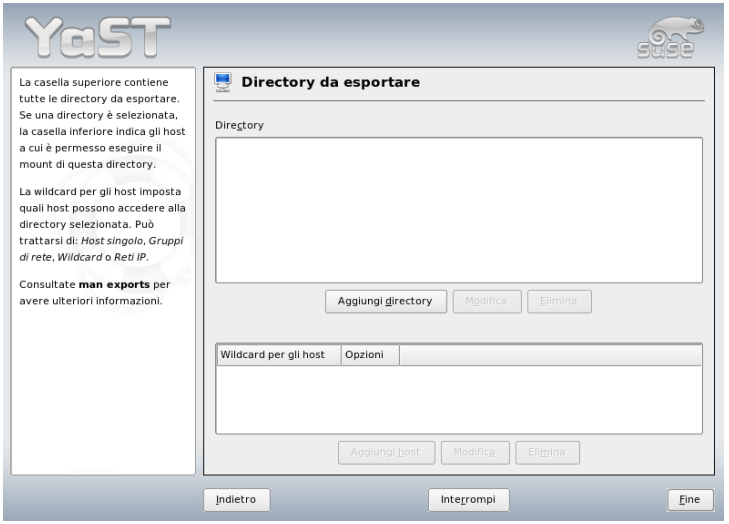

Figura 26.3: *Configurare un server NFS con YaST*

Ogni directory da esportare ha bisogno di una riga che descriva quali computer possano accedervi ed in che modo. Anche tutte le sottodirectory di un indirizzario esportato vengono esportate automaticamente. I computer che possono accedervi vengono solitamente indicati coi propri nomi (compreso il nome di dominio), ma è anche possibile usare dei simboli jolly `*` e `?`, che conosciamo dalla bash. Se non indicate alcun nome di host, saranno tutti i computer ad avere accesso a questa directory (con i diritti indicati).

I permessi con i quali una directory viene esportata sono riportati nella lista tra parentesi, dopo il nome del computer. I principali permessi di accesso sono descritti nella tabella successiva:

Tabella 26.1: *Permessi di acceso per directory esportate*

Opzioni	Significato
`ro`	File system viene esportato solo con permesso di lettura (Default).

`rw`	File system viene esportato solo con permesso di lettura e scrittura.
`root_squash`	Questa opzione fa sì che l'utente `root` del computer in questione non disponga dei tipici diritti di `root` per questo file system. Per realizzare ciò, gli accessi con l'user–ID `0` (`root`) vengono eseguiti con l' user-ID `65534`, che dovrebbe essere attribuito all'utente `nobody` (default).
`no_root_squash`	I permessi di accesso di root restano invariati.
`link_relative`	Questa opzione converte i link assoluti e simbolici (ovvero tutti quelli che iniziano con `/`) in una sequenza di `../`. É un'opzione utile solo quando viene montato l'intero file system di un computer (default).
`link_absolute`	I link simbolici restano invariati.
`map_identity`	Sul client, vengono usate le stesse ID dell'utente come sul server (default).
`map_daemon`	Client e server non hanno le stesse user–ID. Con questa opzione, nfsd riceve l' istruzione di creare una tabella di conversione per le user–ID, a condizione che abbiate attivato il demone *ugidd*.

Il vostro file `exports` avrà un aspetto simile a quanto riportato nell'esempio 26.1 in questa pagina. Il file `/etc/exports` viene letto da mountd e nfsd. Se viene modificato, sia mountd che nfsd devono essere riavviati in modo da assumere la modifica apportata. Il modo più semplice per realizzare ciò è quello di eseguire il comando `rcnfsserver restart`.

Esempio 26.1: */etc/exports*

```
 #
# /etc/exports
#
/home            sole(rw)   venere(rw)
/usr/X11         sole(ro)   venere(ro)
/usr/lib/texmf   sole(ro)   venere(rw)
/                terra(ro,root_squash)
/home/ftp        (ro)
# End of exports
```

DHCP

Il cosiddetto “Dynamic Host Configuration Protocol” permette di assegnare i parametri di configurazione della rete ai singoli host tramite un server centrale, senza dover quindi configurare ogni singolo host presente sulla rete. Un client configurato tramite DHCP non dispone di indirizzi statici, ma viene configurato in modo automatico secondo le indicazioni del server DHCP.

Il server identifica i client in base al loro indirizzo di hardware della scheda di rete e quindi potrà assegnare loro costantemente le stesse impostazioni, come pure allocare ai client, che ne fanno richiesta, degli indirizzi in modo dinamico presi da un pool di indirizzi. In questo caso, il server DHCP provvederà a far sì che ad ogni richiesta venga assegnato al client lo stesso indirizzo anche per lunghi periodi di tempo — naturalmente, questo non funziona se nella rete vi sono più sistemi che indirizzi disponibili.

Un amministratore di sistema può quindi trarre vantaggio da DHCP in due modi diversi. Da un lato è possibile modificare comodamente gli indirizzi di rete e la configurazione intervenendo sul file di configurazione del server DHCP senza dover configurare singolarmente i vari client, e dall'altro, in particolar modo i client che si vanno ad aggiungere sulla rete possono essere integrati facilmente nella rete, assegnando loro un indirizzo IP preso dall'intervallo (pool) degli indirizzi. Anche per i portatili utilizzati continuamente in reti diverse è certamente una soluzione interessante ricevere da un server DHCP di volta in volta i parametri di rete appropriati.

Oltre all'indirizzo IP e alla maschera di rete, vengono comunicati al client anche il nome dell' host e del dominio, il gateway da utilizzare e gli indirizzi dei server dei nomi. Inoltre, possono venire configurati centralmente anche molti altri parametri come p.es. un time server da cui richiedere l'ora attuale o un server di stampa.

27.1 Configurare DHCP con YaST

All'avvio del modulo YaST invoca un assistente di configurazione. Concluso il procedimento configurativo avrete a vostra disposizione un semplice server DHCP sulla vostra rete.

Selezione dell'interfaccia di rete Innanzitutto YaST rileva le interfacce di rete del vostro sistema. Selezionate dall'elenco quella sulla quale il server DHCP debba mettersi in ascolto e stabilite tramite l'opzione 'Apri firewall per interfacce selezionate' se il firewall debba essere aperto per questa interfaccia (si veda la figura 27.1 nella pagina successiva).

Impostazioni generali Negli altri campi di immissione stabilite le informazioni di rete che ogni client amministrato da questo server DHCP debba ricevere: nome del dominio, indirizzo del server dell'ora, indirizzo del server dei nomi primario e secondario, indirizzo del server di stampa e server WINS (in

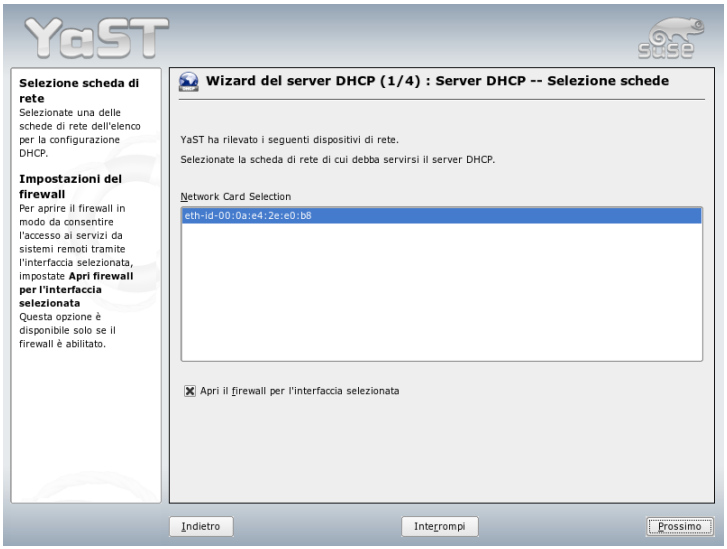

Figura 27.1: *Server DHCP: selezione dell'interfaccia di rete*

reti eterogenee con client Windows e Linux) nonché l'indirizzo del gateway e la scadenza dell'indirizzo dato in affitto (si veda la figura 27.2 nella pagina seguente).

DHCP dinamico Si prosegue con la configurazione della allocazione dinamica degli indirizzi IP ai client connessi. A tal fine stabilite un intervallo di indirizzo IP nel quale si trovano gli indirizzi da assegnare. Tutti gli indirizzi devono appartenere alla stessa maschera di rete. Stabilite infine la scadenza degli indirizzi durante la quale il client può mantenere l'indirizzo senza dover fare "richiesta" di prolungamento della scadenza. Inoltre stabilite facoltativamente il tempo massimo per il quale un determinato indirizzo IP sul server venga riservato per un determinato client (si veda la figura 27.3 a pagina 483).

Concludere la configurazione e selezionare il modo di avvio
Conclusa la terza parte dell'iter configurativo, giungete all'ultima finestra, nella quale stabilite le opzioni di avvio del server DHCP, ad esempio se il server DHCP debba essere avviato automaticamente al boot del sistema

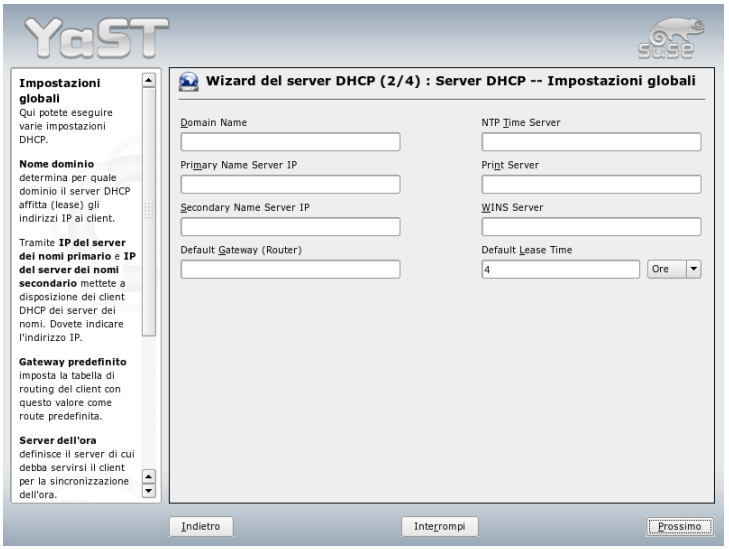

Figura 27.2: *Server DHCP: impostazioni generali*

('Avvia server DHCP al boot') o se va lanciato manualmente all'occorrenza, ad es. per eseguire dei test), ('Avvia server DHCP manualmente'). Cliccando su 'Fine' portate a termine il processo configurativo del server (si veda la figura 27.4 a pagina 484).

27.2 I pacchetti software DHCP

SUSE LINUX vi offre sia un server DHCP che due pacchetti client. Il server DHCP dhcpd rilasciato dall'ISC (Internet Software Consortium) mette a disposizione i servizi server; come client potete utilizzare sia dhclient , rilasciato dall'ISC che il cosiddetto "DHCP Client Daemon" contenuto nel pacchetto `dhcpcd`.

Il `dhcpcd` installato come standard in SUSE LINUX è molto semplice da gestire, e viene lanciato automaticamente all'avvio del sistema per rilevare il server DHCP. Se la cava senza un file di configurazione e normalmente non è necessario intervenire sulla configurazione. Per scenari più complessi, si può ricor-

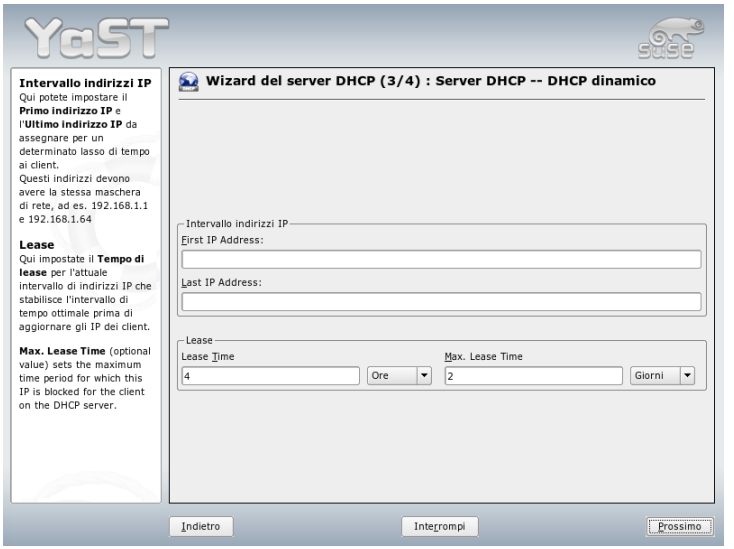

Figura 27.3: *Server DHCP: DHCP dinamico*

rere al dhclient dell'ISC che potete amministrare tramite il file di configurazione `/etc/dhclient.conf`.

27.3 Il server DHCP dhcpd

Il *Dynamic Host Configuration Protocol Daemon* è il cuore di ogni sistema DHCP che dà in "affitto" indirizzi e ne sorveglia l'uso in base a quanto stabilito nel file di configurazione `/etc/dhcpd.conf`. Tramite i parametri e i valori lì definiti, l'amministratore di sistema dispone di numerosi mezzi per impostare il comportamento del server DHCP secondo le sue preferenze.

Esempio di un semplice file `/etc/dhcpd.conf`:

Esempio 27.1: *Il file di configurazione /etc/dhcpd.conf*

```
default-lease-time 600;          # 10 minutes
max-lease-time 7200;             # 2  hours
```

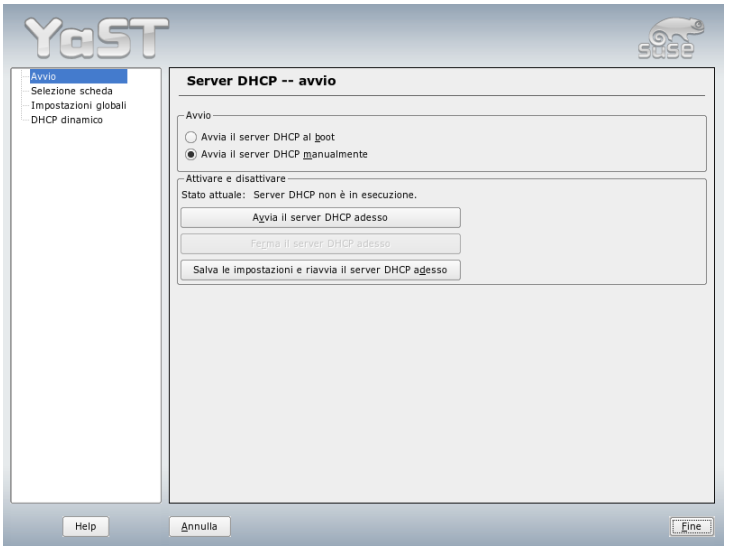

Figura 27.4: *Server DHCP: avvio*

```
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;
 }
```

Questo semplice file di configurazione è sufficiente affinché DHCP sia in grado di attribuire indirizzi IP nella vostra rete. Fate specialmente attenzione ai punti e virgola alla fine di ogni riga; senza di essi, dhcpd non si avvierà!

Come vedete, il nostro esempio si lascia suddividere in tre blocchi. Nel primo blocco viene definito di default per quanti secondi un indirizzo IP venga da-

to in "affitto" ad un computer richiedente, prima che questi cerchi di ottenere una proroga (`default-lease-time`). Qui viene anche indicato il periodo di tempo massimo per il quale un computer può mantenere il numero IP assegnatogli dal server DHCP, senza dover richiedere una dilazione di tempo (`max-lease-time`).

Nel secondo blocco vengono definiti globalmente alcuni parametri di rete fondamentali:

- Con `option domain-name` viene definito il dominio di default della vostra rete.
- Con `option domain-name-server` possono venire indicati fino a tre server DNS che devono venire utilizzati per la risoluzione di indirizzi IP in nomi di host (e viceversa). E' consigliabile che sul vostro sistema o sulla vostra rete, fosse già in esecuzione un server dei nomi che tenesse in serbo anche un nome di host per indirizzi dinamici e viceversa. Ulteriori informazioni riguardanti la configurazione di un proprio server dei nomi si veda il capitolo 24 a pagina 445.
- `option broadcast-address` stabilisce quale indirizzo broadcast debba usare il computer richiedente.
- `option routers` stabilisce dove debbano venire inviati quei pacchetti di dati che in base all'indirizzo dell' host mittente e dell' host meta nonché della maschera della sottorete non possono venire recapitati nella rete locale. Nella maggior parte dei casi, proprio nelle reti di minor dimensione questo router è anche l'anello di connessione per l'Internet.
- `option subnet-mask` indica la maschera di rete da consegnare al client.

Al di sotto di queste impostazioni generali vi è la definizione di un'altra rete con la maschera di sottorete. Infine, va stabilita un'area indirizzi dalla quale il demone DHCP possa attribuire indirizzi ai client che ne fanno richiesta. Nel nostro esempio, gli indirizzi fra `192.168.1.10` e `192.168.1.20` oppure `192.168.1.100` e `192.168.1.200`.

Dopo queste poche righe, dovreste già essere in grado di attivare, con il comando `rcdhcpd start`, il demone DHCP che sarà subito a vostra disposizione. Con `rcdhcpd check-syntax` potete anche far eseguire un breve controllo riguardante la sintassi del file di configurazione. Se inaspettatamente dovessero verificarsi dei problemi di configurazione ed il server dovesse terminare con

un errore invece di avviarsi con un `done`, consultate il file di protocollo del sistema centrale `/var/log/messages`, oppure data un'occhiata alla console 10 (Ctrl-Alt-F10).

In SUSE LINUX il demone DHCP viene lanciato di default, per motivi di sicurezza, in un ambiente chroot. Affinché vengano rilevati i file di configurazione, anch' essi devono essere copiati nel nuovo ambiente. Questo avviene automaticamente con `rcdhcpd start`.

27.3.1 Computer con indirizzo IP statico

Come già accennato all'inizio, con DHCP è possibile assegnare ad un client un determinato indirizzo ad ogni richiesta.

Naturalmente tali esplicite attribuzioni di indirizzi hanno la precedenza sull'attribuzione dinamica di un indirizzo preso dal pool ovvero insieme di indirizzi. Gli indirizzi allocati esplicitamente non hanno una scadenza, come è invece il caso per quelli dinamici, quando non è più disponibile un numero sufficiente di indirizzi liberi e quindi si rende necessaria una riallocazione degli indirizzi.

Per identificare un sistema con un indirizzo *statico*, il dhcpd ricorre al cosiddetto indirizzo hardware: si tratta di un determinato codice unico al mondo composto da sei coppie di ottetti assegnato ad ogni dispositivo di rete, p.es. `00:00:45:12:EE:F4`. Se al file di configurazione dell'esempio 27.1 a pagina 483 viene aggiunta una registrazione come nell'esempio 27.2 in questa pagina, il dhcpd fornirà in ogni caso gli stessi dati al sistema corrispondente.

Esempio 27.2: *Aggiunte al file di configurazione*

```
host  {
hardware ethernet 00:00:45:12:EE:F4;
fixed-address 192.168.1.21;
}
```

La struttura di queste righe è autoesplicativa: come prima cosa viene indicato il nome del sistema da definire (`host` ⟨*nome host*⟩, in questo caso `terra`), e nella riga seguente si indica l'indirizzo MAC. Nei sistemi Linux, potete rilevare questo indirizzo servendovi del comando `ifstatus` accompagnato dal nome della scheda di rete (ad esempio, `eth0`). Può darsi che sia necessario attivare prima la scheda, fatelo con: `ifup  eth0`. Otterrete un output del tipo:

```
link/ether 00:00:45:12:EE:F4
```

Nel nostro esempio, viene assegnato al sistema - la cui scheda di rete possiede l'indirizzo MAC `00:00:45:12:EE:F4` - l'indirizzo IP `192.168.1.21` ed il nome host terra. Oggigiorno, come tipo di hardware viene generalmente usato `ethernet`, ma viene anche supportato `token-ring`, usato per la maggior parte con sistemi IBM.

27.3.2 Particolarità di SUSE LINUX

Per ragioni di sicurezza in SUSE è contenuta la patch "non-root/chroot" di Ari Edelkind per il server DHCP ISC che permette a dhcpd di girare come utente `nobody` in un ambiente "chroot" (`/var/lib/dhcp`). Il file di configurazione `dhcpd.conf` deve trovarsi in `/var/lib/dhcp/etc`; lo script di inizializzazione lo copia automaticamente in tale directory all'avvio.

Questa funzionalità si lascia gestire tramite le registrazione contenute nel file `/etc/sysconfig/dhcpd`. Per continuare ad eseguire il dhcpd senza ambiente chroot, impostate la variabile `DHCPD_RUN_CHROOTED` nel file `/etc/sysconfig/dhcpd` su "no"

Affinché il dhcpd sia in grado di risolvere dei nomi host anche in un ambiente chroot si dovranno copiare inoltre i seguenti file di configurazione:

- `/etc/localtime`
- `/etc/host.conf`
- `/etc/hosts`
- `/etc/resolv.conf`

Ecco perché all'avvio dello script di inizializzazione anche questi file vengono copiati in `/var/lib/dhcp/etc/`. Questi file vanno tenuti aggiornati se vengono modificati in modo dinamico da script del tipo `/etc/ppp/ip-up`. Se nel file di configurazione si utilizzano solo indirizzi IP al posto di nomi host, non dovrebbero sorgere delle difficoltà.

Se il vostro tipo di configurazione richiede che vengano copiati nell'ambiente chroot in aggiunta determinati file, potete indicarli accanto al parametro `DHCPD_CONF_INCLUDE_FILES` nel file `etc/sysconfig/dhcpd`. Affinché il demone dhcp possa continuare la sua attività di log nell'ambiente chroot, anche se viene riavviato il demone syslog, bisogna aggiungere il parametro `"-a /var/lib/dhcp/dev/log"` alla variabile `SYSLOGD_PARAMS` in `/etc/sysconfig/syslog` .

27.4 Ulteriori fonti di informazione

Per delle ulteriori informazioni dettagliate, visitate ad.es. il sito dell'*Internet Software Consortium* (`http://www.isc.org/products/DHCP/`. Inoltre vi sono le pagine di manuale, in particolar modo `dhcpd`, `dhcpd.conf`, `dhcpd.leases`, and `dhcp-options`.

28

Sincronizzare l'orario con xntp

NTP (Network Time Protocol) è un protocollo preposto alla sincronizzazione dell'ora del sistema tramite rete. Una macchina può ottenere l'ora esatta da un server che funge da origine affidabile dell'ora. Comunque vi è anche la possibilità che una macchina funga da origine dell'ora per altri computer presenti sulla rete. L'obiettivo è quello di avere l'orario assoluto e la sincronizzazione dell'ora di sistema di tutte le macchine che compongono una rete.

L'ora esatta svolge un ruolo di primo piano per tanti processi di sistema. L'orologio hardware (BIOS) integrato spesso comunque si rivela di non essere all'altezza delle richieste avanzate da applicazioni come banca dati. Intervenire in modo continuato manualmente sull'orario del sistema potrebbe causare delle serie difficoltà, per fare un esempio un salto brusco all'indietro dell'ora causa incide sul corretto funzionamento di applicazioni critiche. In una rete di solito è necessario sincronizzare l'ora di sistema di tutte le macchine, comunque degli adattamenti manuali non rappresentano la soluzione ideale. xntp mette a disposizione un meccanismo che assolve questo compito. L'ora del sistema viene continuamente regolata tramite dei server dell'ora affidabili in esecuzione sulla rete. Inoltre consente di amministrare dei dispositivi che scandiscono l'ora di riferimento, come ad esempio orologi a controllo radio.

28.1 Configurazione nella rete

xntp è preconfigurato in modo che solo l'orario del sistema locale funge da ora di riferimento. Fare riferimento all' ora scandita dal BIOS rappresenta comunque una soluzione di ripiego nel caso di non disponibilità di una fonte dell'orario di maggior precisione. Il modo più semplice di utilizzare dei server dell'ora nella rete consiste nell'impostazione di cosiddetti parametri "server". Se nella rete vi è un server dell'orario che ad esempio porta il nome `ntp.example.com`, potete immettere il nome del server in `/etc/ntp.conf` aggiungendo il seguente rigo: `server ntp.example.com`. Ulteriori server dell'ora si aggiungono immettendo semplicemente ulteriori righe con la parola chiave "server". Dopo aver inizializzato xntpd con il comando `rcxntpd start`, passa ca. un'ora prima che l'ora si stabilizzi e che venga creato il file "drift" per correggere l'orario del sistema locale. Il file "drift" a lungo termine comporta il vantaggio che non appena viene acceso il computer, si sa di quanto l'orario del sistema si discosta. Quindi si potrà procedere immediatamente alla correzione dell'orario per cui si ha una elevata stabilità dell'orario del sistema.

Vi sono due modi per utilizzare NTP come client: inviare ad intervalli regolari delle richieste riferite all'orario ad un server. Se si ha un numero elevato di client, questo approccio comporta un elevato carico di lavoro per il server; oppure il client aspetta che vengano inviati dei broadcast NTP da parte dei server dell'ora. Lo svantaggio di questo approccio consiste nel fatto che si ignora la bontà del server e se il server invia delle informazioni errate sorgeranno delle serie difficoltà.

Se nella vostra rete il server dell'ora invia dei broadcast, non è necessario più il nome del server. In questi casi immettete il rigo `broadcastclient` nel file di configurazione `/etc/ntp.conf`. Se preferite ricorrere solo a uno o più server dell'ora noti, immettete i rispettivi nomi nel rigo che inizia con `servers`.

28.2 Impostare un orario di riferimento locale

Il pacchetto software xntp contiene anche dei driver che permettono di impostare l'ora di riferimento locale. Un elenco dei dispositivi per la scansione del tempo supportati è reperibile nel pacchetto `xntp-doc` nel file `/usr/share/doc/packages/xntp-doc/html/refclock.htm`. Ogni driver ha un numero. La configurazione di xntp in sé avviene tramite dei cosiddetti pseudo IP. I dispositivi che scandiscono l'ora vanno registrati nel file `/etc/ntp.conf`, come se fossero disponibili nella rete. A riguardo gli vengono assegnati degli indirizzi IP particolari simili a: `127.127.t.u`. Il valore `t` sta per il tipo di dispositivo e indica il driver da utilizzare e `u` sta per unità e indica l'interfaccia utilizzata.

I singoli driver di solito hanno dei parametri speciali che descrivono la configurazione in modo più dettagliata. Nel file `/usr/share/doc/packages/xntp-doc/html/driverNN.htm` (laddove `NN` prende il posto del numero del driver) trovate delle indicazioni sul tipo di orologio in questione. Per orologi del "tipo 8" (orologio a controllo radio, interfaccia seriale) ad esempio è necessario indicare un ulteriore cosiddetto mode che specifica meglio l'orologio. Il modulo "Conrad DCF77 receiver" ad esempio presenta il "mode 5". Affinché questo orologio funga da riferimento, specificate la parola chiave `prefer`. Il rigo `server` completo per "Conrad DCF77 receiver module" sarebbe quindi:

```
server 127.127.8.0 mode 5 prefer
```

Per gli altri dispositivi del genere seguite lo stesso schema. La documentazione su xntp la trovate dopo aver installato il pacchetto `xntp-doc` nella directory `/usr/share/doc/packages/xntp-doc/html`. Il file `/usr/share/doc/packages/xntp-doc/html/refclock.htm` offre dei link che rimandano alle driver pages che descrivono i parametri dei driver.

28.3 Configurazione di un client NTP tramite YaST

Accanto alla configurazione manuale di xntp appena descritta, SUSE LINUX consente di impostare client NTP tramite YaST. Potete scegliere tra configurazione rapida semplice e configurazione complessa. Nelle sezioni seguenti ci occuperemo di entrambe le possibilità.

28.3.1 Configurazione rapida di un client NTP

Il processo di configurazione semplice di un client NTP si compone di solo due finestre. Nella prima stabilite il modo di avviamento di xntpd ed il server di riferimento. Per lanciare il demone automaticamente all'avvio del sistema, cliccate su 'All'avvio del sistema'. Per rilevare un server dell'ora appropriato sulla rete, cliccate su 'Seleziona' e arriverete alla seconda finestra per la selezione del server.

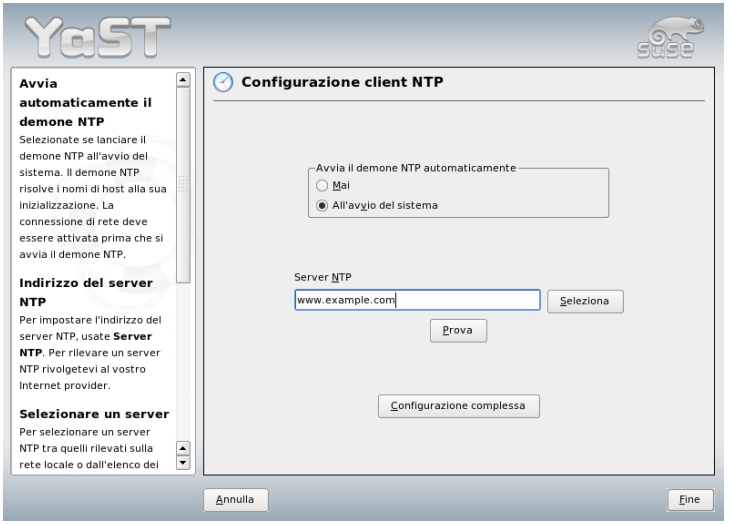

Figura 28.1: *YaST: configurazione del client NTP*

Nella finestra di selezione del server stabilite innanzitutto se preferite una sincronizzazione dell'ora tramite un server della propria rete (radio bottone 'Rete

locale') o se debba essere contattato un server dell'ora sull'Internet (radio bottone 'Server NTP pubblico'). Nel caso di un server dell'ora locale cliccate su 'Cerca' per inizializzare una richiesta SLP di server dell'ora disponibili sulla vostra rete. Dall'elenco risultante selezionate il server adatto e uscite dalla finestra con 'OK'. Per selezionare un server dell'ora pubblico, selezionate nella finestra 'Server NTP pubblico' il vostro paese (fuso orario) e dall'elenco risultante il server adatto. Concludete la configurazione con 'OK' seguito da 'Fine' dopo aver accertato con'Prova' che il server risulti essere indirizzabile.

28.3.2 Configurazione complessa del client NTP

Per giungere alla configurazione complessa del client NTP, selezionate 'Configurazione complessa' nel dialogo iniziale del 'Client NTP' (si veda la figura 28.1 a fronte), dopo aver selezionato il modo di avviamento, come descritto per la configurazione rapida.

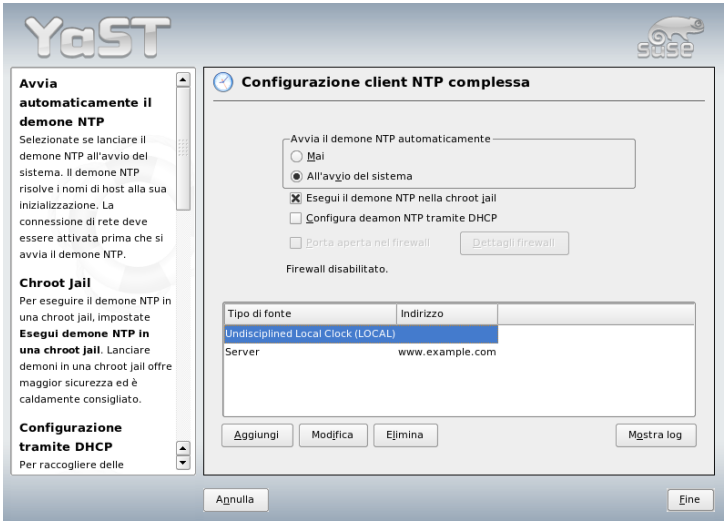

Figura 28.2: *YaST configurazione complessa del client NTP*

Nella finestra 'Configurazione complessa del client NTP' determinate se xntpd debba essere lanciato in una gabbia di chroot. In tal modo si incrementa il livello

di sicurezza nel caso di un attacco tramite xntpd, visto che l'aggressore non potrà compromettere l'intero sistema. Inoltre, tramite 'Configura demone NTP tramite DHCP' potete impostare il client NTP in modo che venga ottenga l'elenco dei server NTP disponibili sulla rete tramite DHCP.

Nella parte inferiore della finestra vengono elencati il server ed altre le fonti dell'ora a cui potrà rivolgersi il client. Potete editare questo elenco tramite 'Aggiungi', 'Modifica' e 'Elimina'. Tramite 'Per esperti..' avete modo di visionare i file di log del vostro client o di adeguare il firewall alla configurazione del client NTP.

Per aggiungere una nuova fonte oraria, cliccate su 'Aggiungi'. Nella finestra successiva, selezionate il tipo di fonte tramite la quale debba realizzarsi la sincronizzazione dell'ora. Potete scegliere tra le seguenti opzioni:

Server Successivamente selezionate il server NTP (come descritto nella sezione 28.3.1 a pagina 492) e abilitate l'opzione 'Utilizza per sincronizzazione iniziale' per realizzare la sincronizzazione tra server e client durante il boot. Negli altri campi potete indicare ulteriori opzioni per xntpd. Maggiori informazioni sono reperibili sotto `/usr/share/doc/packages/xntp-doc`.

Peer Un peer è una macchina con la quale si instaura un rapporto simmetrico: esso funge sia da server dell'ora che da client. Se il processo debba avvenire tramite un peer della stessa rete al posto di un server, indicate l'indirizzo del sistema. Per il resto la finestra è identica a quella per il 'server'.

Orologio a controllo radio Se sul vostro sistema disponete di un dispositivo del genere e intendete utilizzarlo per sincronizzare l'ora, indicate in questa finestra il tipo di orologio, numero di unità e nome di dispositivo nonché ulteriori opzioni. Tramite 'Calibrare driver' eseguite la configurazione mirata del rispettivo driver. Informazioni dettagliate sul modo di utilizzare un orologio locale a controllo radio sono reperibili sotto `/usr/share/doc/packages/xntp-doc/html/refclock.htm`.

Broadcasting Informazioni e richieste riguardanti l'ora possono essere inviati anche via broadcast nella rete. Nel presente dialogo indicate gli indirizzi meta per i broadcast. Non abilitate questa opzione se non disponete di una fonte dell'ora affidabile come ad es. un orologio a controllo radio.

Accettare pacchetti broadcast Se il vostro client debba ottenere le sue informazioni tramite broadcast, inserite nel presente dialogo l'indirizzo dal quale accettare i corrispondenti pacchetti.

29

LDAP — Un servizio directory

LDAP (Lightweight Directory Access Protocol) è un insieme di protocolli ideato per l'accesso e la manutenzione di directory di informazione. LDAP può svolgere diverse funzioni, amministrare utenti e gruppi, la configurazione di sistema o gli indirizzi. In questo capitolo presentiamo gli aspetti basilari di LDAP, il suo modo di funzionare e il modo di gestire dei dati LDAP tramite YaST.

In ambienti di lavoro collegati in rete è determinante che le informazioni importanti siano tenute in serbo in modo strutturato e che siano reperibili immediatamente. Questo problema viene risolto da un servizio directory, il quale alla stregua delle pagine gialle (ingl. Yellow Pages), che conosciamo dalla vita di tutti i giorni, contiene le informazioni richieste in una forma ben strutturata, di facile consultazione ed immediatamente individuabili.

Nel caso ideale vi è un server centrale contenente i dati in una determinata directory che li distribuisce ai client nella rete tramite un protocollo particolare. I dati dovrebbero essere strutturati in modo che una gamma quanto vasta possibile di applicativi possa accedervi. In tal modo non è necessario che ogni tool per calendari o e-mail client disponga di una propria banca dati, ma potrà accede ad uno stock di dati gestiti centralmente. Questo ridurrebbe notevolmente il numero degli interventi di natura amministrativa per le informazioni in questione. Un protocollo aperto e standardizzato come LDAP assicura che una gamma quanto vasta possibile di applicazioni client possa accedere ai dati richiesti.

In questo contesto una directory assume il ruolo di una specie di banca dati ideata e ottimizzata sotto il punto di vista della sua accessibilità e idoneità per consentire una consultazione immediata:

- Per poter realizzare un numero considerevole di accessi in lettura (contemporanei), l'accesso in scrittura viene limitato ai pochi aggiornamenti eseguiti dall'amministratore. Le banche dati si distinguono per la loro caratteristica di recepire in tempi brevi un volume di dati quanto vasto possibile.
- Visto il numero ridotto degli accessi in scrittura sono solitamente dei dati possibilmente *statici* ad essere amministrati tramite un servizio directory, mentre i dati di una banca dati convenzionale sono di solito *di natura dinamica* visto che cambiano frequentemente. Per fare un esempio, l'elenco dei numeri telefonici dei dipendenti non cambierà così spesso come i dati del reparto di contabilità.
- Nel caso di dati statici l'aggiornamento dei set di dati esistenti avviene raramente; nel caso di dati dinamici, soprattutto quando si tratta di set di dati relativi a conti bancari e contabilità, è la consistenza dei dati ad assumere un ruolo di primo piano. Se una somma va detratta da una parte e aggiunta ad un'altra, le due operazioni devono avvenire contemporaneamente, cioè tramite una sola "transazione" per assicurare la consistenza dei dati nel loro insieme. Banche dati supportano queste transazioni, directory no. Nel caso delle directory comunque inconsistenze temporanee sono accettabili.

Lo scopo di un servizio directory come LDAP non è tanto quello di supportare complessi meccanismi di aggiornamento ed interrogazione; si tratta piuttosto di consentire agli applicativi, che accedono a questo servizio, di accedervi in modo quanto semplice e veloce possibile.

Esistono tanti servizi directory, e non solo nel mondo Unix, ad esempio NDS di Novell, ADS di Microsoft, Banyans Street Talk e lo standard OSI X.500. Originariamente LDAP è stato concepito come versione 'snella' di DAP (ingl. Directory Access Protocol), sviluppato per l'accesso a X.500. Lo standard X.500 regola la disposizione gerarchica delle voci della directory.

LDAP è stato per così dire alleggerito di alcune funzionalità di DAP, può essere utilizzato cross-plattform e fa un uso parsimonioso delle risorse, senza dover rinunciare alla disposizione gerarchica delle voci di X.500. Grazie a TCP/IP, diventa più semplice interfacciare applicazione e servizio LDAP.

Nel frattempo si è proseguito nello sviluppo di LDAP, e sempre più spesso LDAP viene implementato come soluzione stand-alone senza supporto per X.500. Con LDAPv3 (la versione del protocollo a vostra disposizione una volta installato il pacchetto `openldap2`, LDAP supporta i cosiddetti *referrals* che permettono di realizzare banche dati dislocate. Nuovo è anche il fatto che viene utilizzato SASL (ingl. Simple Authentication and Security Layer) quale strato di autenticazione e di sicurezza.

L'uso di LDAP non si limita alla possibilità di inviare delle richieste ai server X.500 come era invece previsto all'inizio. Con slapd esiste un server open source in grado di archiviare le informazioni degli oggetti in una banca dati locale. Questo server viene completato da slurpd preposto alla replica di più server LDAP.

Il pacchetto `openldap2` è composto principalmente di due programmi.

slapd Un server LDAPv3 stand-alone che amministra le informazioni degli oggetti in una banca dati basata su BerkeleyDB.

slurpd Questo programma replica le modifiche apportate ai dati del server LDAP locale agli altri server LDAP presenti nella rete.

Tool aggiuntivi per l'amministrazione del sistema
`slapcat`, `slapadd`, `slapindex`

29.1 LDAP vs. NIS

Un amministratore di sistema Unix utilizza solitamente il servizio NIS per la risoluzione dei nomi e la distribuzione dei dati nella rete. Un server centrale

distribuisce ai client presenti sulla rete i dati di configurazione dei file e directory di `/etc`: `group`, `hosts`, `mail`, `netgroup`, `networks`, `passwd`, `printcap`, `protocols`, `rpc` e `services`. L'amministrazione di questi semplici file di testo risulta essere semplice, ma il tutto diventa più complicato quando si tratta di gestire una maggior quantitativo di dati, visto che manca ogni tipo di strutturazione. NIS è stato ideato solo per piattaforme Unix, quindi non può essere utilizzato per l'amministrazione centralizzata dei dati in una rete eterogenea.

LDAP invece non si limita a reti puramente Unix. Server Windows (a partire da Windows 2000) supportano LDAP quale servizio di directory. Anche Novell offre il servizio LDAP. Inoltre, LDAP sa fare più di quanto riferito finora.

LDAP può essere utilizzato per qualsiasi struttura di dati da amministrare centralmente. Ecco alcuni esempi:

- In sostituzione di un server NIS
- Mail routing (postfix, sendmail)
- Rubriche per mail client come Mozilla, Evolution, Outlook, ...
- Amministrazione delle descrizioni delle zone di un server dei nomi BIND9

e l'elenco non si esaurisce qui, visto che al contrario di NIS, LDAP è scalabile. La chiara struttura gerarchica dei dati è di aiuto quando si tratta di amministrare una quantità considerevole di dati.

29.2 Struttura dell'albero directory di LDAP

Una directory LDAP ha una struttura ad albero. Tutte le registrazioni (dette oggetti) nella directory hanno un posizione ben definita all' interno di questa gerarchia. Questo gerarchia porta il nome di *Directory Information Tree* abbreviato con DIT. Il percorso completo che porta alla registrazione richiesta viene chiamato *Distinguished Name* abbreviato con DN. I singoli nodi che portano alla registrazione richiesta vengono chiamati *Relative Distinguished Name* o RDN. Gli oggetti sono in sostanza di due tipi:

Container Questi oggetti contengono altri oggetti. Queste classi di oggetti sono `root` (radice immaginaria dell'albero delle directory), `c` (ingl. country), `ou` (ingl. OrganizationalUnit) e `dc` (ingl. domainComponent). Questo modello ricorda quello delle directory in un file system.

Nodi intermedi o foglie Questi oggetti si trovano alla fine di un ramo. Al di sotto non vi sono altri oggetti. Esempi: `Person`,`InetOrgPerson` oppure `groupofNames`.

In cima alla gerarchia abbiamo una radice `root`. Seguono poi per esempio `c` (ingl. country), `dc` (ingl. domain component) oppure `o` (ingl. organization). Le relazioni che intercorrono all'interno di un albero di directory LDAP vengono illustrate nel seguente esempio (si veda la figura 29.1 in questa pagina).

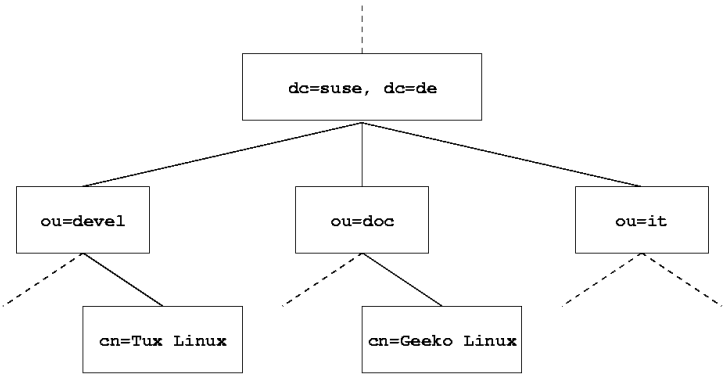

Figura 29.1: *Struttura di una directory LDAP*

L'intera figura comprende un *Directory Information Tree* esempio. Le registrazioni (ingl, entries) sono riportate su tre livelli. Ogni registrazione corrisponde nella figura ad un quadretto. Il *Distinguished Name* completo e valido per il dipendente SuSE fittizio `Geeko Linux` è `cn=Geeko Linux,ou=doc,dc=suse,dc=de`, che viene composto aggiungendo l'RDN `cn=Geeko Linux` al DN della registrazione precedente `ou=doc,dc=suse,dc=de`.

L'impostazione globale, quale tipo di oggetti debba essere archiviato nel DIT si realizza tramite uno *schema* . Il tipo di un oggetto viene stabilito tramite la *Classe degli oggetti*. La classe degli oggetti determina quali attributi *debbano* oppure *possano* essere assegnati all'oggetto in questione. Uno schema deve quindi contenere le definizioni di tutte le classi di oggetto e di tutti gli attributi utilizzati nello scenario di impiego desiderato. Esistono alcuni schemi diffusi (si veda RFC 2252 e 2256). Comunque, potete anche generare degli schemi vostri oppure utilizzare diversi schemi che si completano a vicenda, se richiesto dall'ambiente in cui viene utilizzato il server LDAP.

La tabella 29.1 in questa pagina offre una rassegna delle classi di oggetto utilizzate nell'esempio prese da `core.schema` e `inetorgperson.schema` con gli attributi necessari e valori di attributo adatti.

Tabella 29.1: *Classi di oggetto e attributi frequenti*

Classe di oggetto	Significato	Registrazione esempio	Attributi richiesti
dcObject	*domainComponent* (parti del nome del dominio)	suse	dc
organizationalUnit	*organizationalUnit* (Unità di organizzazione)	doc	ou
inetOrgPerson	*inetOrgPerson* (Dati di persone per Intranet/Internet)	Geeko Linux	sn e cn

Nell'output dell'esempio 29.1 in questa pagina vedete un'estratto di una direttiva schema con degli utili commenti.

Esempio 29.1: *Estratto dal schema.core (a scopo esplicativo sono state numerate le righe)*

```
...
#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) )
...
```

Come esempio abbiamo il tipo di attributo `organizationalUnitName` e la classe di oggetto relativa `organizationalUnit`. Nel primo rigo abbiamo il

nome dell'attributo, OID (*Object Identifier*) (numerico) univoco e l'abbreviazione dell'attributo.

Il rigo 2 viene introdotto da `DESC`, una breve descrizione dell' attributo a cui qui segue l'indicazione del relativo RFC da cui è stata presa la definizione. `SUP` nel rigo 3 rimanda ad un tipo di attributo superiore, a cui appartiene questo attributo.

La definizione della classe di oggetto `organizationalUnit` inizia al rigo 4 come per la definizione dell'attributo con un OID ed un nome per la classe di oggetto. Nel rigo 5 abbiamo una breve descrizione della classe di oggetto. Con la registrazione `SUP top` il rigo 6 vi indica che questa classe di oggetto non è subordinata ad un'altra classe di oggetto. Nel rigo 7 vengono indicati dopo `MUST` tutti i tipi di attributo che *devono* essere utilizzati in un oggetto del tipo `organizationalUnit`. Nel rigo 8, dopo `MAY` avete l'elenco dei tipi di attributo che *possono* essere utilizzati con questa classi di oggetti.

Per una introduzione molto valida all'uso degli schemi rimandiamo alla documentazione su OpenLDAP che trovate nel vostro sistema installato sotto `/usr/share/doc/packages/openldap2/admin-guide/index.html`.

29.3 Configurazione server con slapd.conf

`/etc/openldap/slapd.conf` è il file di configurazione del vostro server LDAP, una volta installato il sistema. Di seguito illustreremo brevemente le singole registrazioni e gli adattamenti necessari. Tenete presente che le registrazioni con un # all'inizio non sono abilitate. Per abilitarle dovete eliminare questo segno di commento.

29.3.1 Direttive globali in slapd.conf

Esempio 29.2: *slapd.conf: direttiva include per schemi*

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/inetorgperson.schema
```

Con questa prima direttiva in `slapd.conf` viene specificato lo schema secondo il quale è organizzata la vostra directory LDAP (si veda l'output dell'esempio 29.2 nella pagina precedente). La registrazione `core.schema` è obbligatoria. Se dovessero servirvi ulteriori schemi, aggiungeteli a questa direttiva (nell' esempio è stato aggiunto `inetorgperson.schema`). Altri schemi disponibili sono reperibili nella directory `/etc/openldap/schema/`. Se intendete sostituire NIS tramite un servizio LDAP analogo, integrate qui gli schemi `cosine.schema` e `rfc2307.schema`. Per ulteriori informazioni su questa problematica, consultate la documentazione OpenLDAP fornita a corredo.

Esempio 29.3: *slapd.conf: pidfile ed argsfile*

```
pidfile /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args
```

Questi due file contengono il PID (ingl. process id) ed alcuni argomenti con i quali lanciare il processo slapd. Non occorre apportare delle modifiche.

Esempio 29.4: *slapd.conf: controllo degli accessi*

```
# 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!
```

Nell'esempio 29.4 in questa pagina vedete la sezione di `slapd.conf` che regola il controllo degli accessi alla directory LDAP sul server. Le impostazioni effettuate nella sezione globale di `slapd.conf` sono effettive, almenoché non vengono sovrascritte da proprie regole di accesso impostate nella sezione della banca dati. Nell'esempio riportato tutti gli utenti hanno accesso in lettura alla directory, ma solo l'amministratore (`rootdn`) ha il permesso di scrittura. Regolare i permessi di accesso sotto LDAP è un processo molto complesso, ecco alcune regole di base utili:

- Ogni regola di accesso è strutturata nel modo seguente:

```
access to <what> by <who> <access>
```

- ⟨*what*⟩ sta per l'oggetto o l'attributo a cui consentite di accedere. Potete proteggere singoli rami dell' albero directory in modo esplicito tramite proprie regole oppure impostare una regola per intere sezioni dell'albero directory tramite espressioni regolari.`slapd` analizzerà le regole nella sequenza riportata nel file di configurazione. Quindi le regole di ordine generale dovrebbero seguire a quelle più specifiche. `slapd` elaborerà la prima regola che giudicherà adeguata ed ignorerà tutte le registrazioni seguenti.
- ⟨*who*⟩ stabilisce chi ha l'accesso a quanto impostato sotto ⟨*what*⟩. Anche qui utilizzando delle espressioni regolari potete semplificarvi le cose. Anche in questo caso non appena `slapd` fa "centro" interromperà l' analisi di ⟨*who*⟩, quindi regole di ordine generale dovrebbero seguire quelle più specifiche. Ecco le registrazioni possibili (si veda la tabella 29.2 in questa pagina):

Tabella 29.2: *Gruppi utenti con permesso di accesso*

Identificatore	Significato
`*`	Tutti gli utenti senza eccezione alcuna
`anonymous`	Utenti non autenticati("anonimi")
`users`	Utenti autenticati
`self`	Utenti connessi all'oggetto meta
`dn.regex=<regex>`	Tutti gli utenti per cui vale questa espressione regolare

- ⟨*access*⟩ specifica il tipo di accesso. Si distingue tra le possibilità riportate nella tabella 29.3 in questa pagina

Tabella 29.3: *Tipi di accesso*

Identificatore	Significato
`none`	Accesso negato
`auth`	Per contattare il server

`compare`	Per l'accesso comparato agli oggetti
`search`	Per l'applicazione di filtri di ricerca
`read`	Permesso di lettura
`write`	Permesso di scrittura

`slapd` confronta il permesso richiesto dal client con quello concesso in `slapd.conf`. Se il permesso lì definito è superiore o uguale a quello richiesto dal client, l'accesso viene concesso. Se invece il client richiede permessi superiori, l'accesso viene negato.

Nell'esempio 29.5 in questa pagina viene illustrato l'output riguardante il controllo degli accessi su cui potete intervenire a piacimento tramite l'uso di espressioni regolari.

Esempio 29.5: *slapd.conf: esempio per il controllo degli accessi*

```
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
```

Questa regola stabilisce che solo il rispettivo amministratore ha l'accesso in scrittura alle registrazioni `ou`. Gli altri utenti autenticati hanno il permesso di lettura ed a tutti gli altri viene negato ogni accesso.

Suggerimento

Impostare le regole di accesso

L'accesso viene negato se non vi è alcuna regola `access to` oppure alcuna direttiva `by` valida. Vengono concessi solo i permessi esplicitamente indicati. Se non viene stabilita alcuna regola, vale il principio: permesso di scrittura per l'amministratore e quello di lettura per tutti gli altri.

Suggerimento

Informazioni dettagliate ed una configurazione esempio dei permessi di accesso LDAP sono reperibili nella documentazione in linea del pacchetto installato `openldap2`.

Oltre alla possibilità di amministrare i controlli di accesso tramite il file di configurazione centrale del server (`slapd.conf`) vi è la possibilità di ricorrere alle ACI (ingl. Access Control Information), per mezzo delle quali le informazioni di accesso per i singoli oggetti possono essere archiviate direttamente nell'albero LDAP. Dato che comunque questo modo di effettuare il controllo degli accessi non è molto diffuso e gli sviluppatori giudicano questa alternativa essere ancora in parte sperimentale, rimandiamo alla relativa documentazione che trovate al sito dedicato al progetto OpenLDAP, ecco l'indirizzo: `http://www.openldap.org/faq/data/cache/758.html`.

29.3.2 Direttive in slapd.conf riguardanti la banca dati

Esempio 29.6: *slapd.conf: direttive riguardanti la banca dati*

```
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
```

Nel primo rigo di questa sezione (si veda l'esempio 29.6 in questa pagina) viene stabilito il tipo di banca dati, nel nostro esempio si tratta di LDBM. Tramite `suffix` nel secondo rigo viene stabilito per quale parte dell' albero di directory LDAP questo server debba essere quello di riferimento. Con `rootdn` si stabilisce chi dispone dell'accesso a scopo amministrativo a questo server. L'utente qui indicato non deve avere una registrazione LDAP o esistere come utente "normale". Con la direttiva `rootpw` impostate la password dell'amministratore. Qui potete immettere al posto di `secret` anche il valore hash della password dell'amministratore generato con `slappasswd`. La direttiva `directory` indica la directory che contiene le directory della banca dati sul server. `index objectClass eq` determina che vi sia un indice delle classi di oggetto. Aggiungete eventualmente dei propri attributi che secondo la vostra esperienza sono quelli maggiormente richiesti. Se di seguito definite delle regole `Access` proprie per la banca dati, saranno queste ad essere applicate al posto delle regole `Access` globali.

29.3.3 Avvio ed arresto del server

Se il server LDAP è stato configurato e tutte le registrazioni desiderate sono state inserite nella directory LDAP secondo il modello riportato di seguito (si veda la sezione 29.4 in questa pagina), avviate il server LDAP come utente `root` immettendo il seguente comando:`rcldap start`. Se volete fermare il server manualmente, immettete `rcldap stop`. Se volete conoscere lo stato di esecuzione del server LDAP, immettete`rcldap status`.

Se volete lanciare e fermare il server all'avvio e allo spegnimento del relativo sistema, utilizzate l'editor dei runlevel di YaST (si veda anche la sezione 7.6 a pagina 171) oppure create i relativi riferimenti degli script di avvio e di arresto sulla riga di comando tramite `insserv` (si veda la sezione 7.5.1 a pagina 169).

29.4 Gestione dei dati nella directory LDAP

OpenLDAP offre all'amministratore una serie di programmi con i quali amministrare i dati nella directory LDAP. Ecco come aggiungere, cancellare, modificare dei dati oppure eseguire delle ricerche.

29.4.1 Aggiungere dei dati in una directory LDAP

Se la configurazione del vostro server LDAP in `/etc/openldap/slapd.conf` è corretta, cioé contiene i valori adatti per `suffix`, `directory`, `rootdn`, `rootpw` ed `index`, potete iniziare con l'immissione dei dati. OpenLDAP utilizza a tal fine il comando `ldapadd`. Per motivi di praticità si consiglia di aggiungere gli oggetti alla banca dati possibilmente in gruppi. A tal fine LDAP supporta il cosiddetto formato LDIF (ingl. LDAP Data Interchange Format). Un file LDIF è un semplice file di testo che può contenere un numero qualsiasi di registrazioni composte da coppie di valori e attributi. Per vedere quali siano le classi di oggetto e gli attributi disponibili, consultate i file schema indicati in `slapd.conf`. Un semplice file LDIF adatto al nostro esempio (la figura 29.1 a pagina 499) assumerebbe il seguente aspetto (si veda l'esempio 29.7 nella pagina successiva):

Esempio 29.7: *Esempio di un file LDIF*

```
# SuSE
dn: dc=suse,dc=de
objectClass: dcObject
objectClass: organization
o: SuSE AG dc: suse

# Dipartimento sviluppo (devel)
dn: ou=devel,dc=suse,dc=de
objectClass: organizationalUnit
ou: devel

# Dipartimento documentazione (doc)
dn: ou=doc,dc=suse,dc=de
objectClass: organizationalUnit
ou: doc

# Dipartimento IT interno (it)
dn: ou=it,dc=suse,dc=de
objectClass: organizationalUnit
ou: it
```

Importante

Codifica dei file LDIF

LDAP utilizza UTF-8 (Unicode). Gli accenti sono quindi codificati correttamente. Utilizzate un editor che supporta UTF-8 (Kate o le versioni recenti di Emacs), altrimenti dovete rinunciare ai caratteri accentuati oppure utilizzare `recode` per ricodificare l'input in UTF-8.

Importante

Salvate il file con l'estensione `.ldif` e passatelo al server con il seguente comando:

```
ldapadd -x -D <dn dell'amministratore> -W -f <file>.ldif
```

La prima opzione `-x` indica che in questo caso si rinuncia all'autenticazione tramite SASL. `-D` caratterizza l'utente che esegue questa operazione; indicate qui il DN valido dell'amministratore come configurato in `slapd.conf`. In questo

esempio concreto si tratta di `cn=admin,dc=suse,dc=de`. Con `-W` eludete l'immissione della password sulla riga di comando (testo in chiaro) e attivate un richiesta di password a parte. La password relativa è stata impostata in precedenza in `slapd.conf` con `rootpw`. `-f` consegna questo nome file. Nell'esempio 29.8 in questa pagina vedete in dettaglio il comando `ldapadd`.

Esempio 29.8: *ldapadd di esempio.ldif*

```
ldapadd -x -D cn=admin,dc=suse,dc=de -W -f esempio.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"
```

I dati utenti dei singoli addetti possono venir raccolti in file LDIF distinti. Nel seguente esempio `tux.ldif` (si veda l'esempio 29.9 in questa pagina) aggiungiamo l'addetto `Tux` alla nuova directory LDAP:

Esempio 29.9: *File LDIF per Tux*

```
# L'addetto 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: +39 1234 567-8
```

Un file LDIF può contenere un numero qualsiasi di oggetti. Potete consegnare al server interi alberi di directory o anche solo parti di esso come ad esempio singoli oggetti. Se dovete modificare più o meno frequentemente i vostri dati, si consiglia di suddividerli in tanti oggetti, in modo da risparmiarvi la ricerca laboriosa degli oggetti da modificare in file voluminosi.

29.4.2 Modificare dati nella directory LDAP

Se dovete modificare dei dati potete utilizzare il tool `ldapmodify`. Il modo più semplice consiste nel modificare prima il relativo file LDIF e di riconsegnare in seguito il file modificato al server LDAP. Per modificare ad esempio il numero telefonico dell'addetto `Tux` da `+39 1234 567-8` a `+39 1234 567-10`, editate il file LDIF come mostrato nell'esempio 29.10 in questa pagina.

Esempio 29.10: *File LDIF modificato: tux.ldif*

```
# L'addetto Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
changetype: modify
replace: telephoneNumber
telephoneNumber: +39 1234 567-10
```

A questo punto importate i dati modificati nella directory LDAP con il seguente comando:

```
ldapmodify -x -D cn=admin,dc=suse,dc=de -W -f tux.ldif
```

Oppure consegnate a `ldapmodify` gli attributi da modificare direttamente sulla riga di comando, procedendo nel modo seguente:

1. Lanciate `ldapmodify` ed immettete la vostra password:

   ```
   ldapmodify -x -D cn=admin,dc=suse,dc=de -W

   Enter LDAP password:
   ```

2. Immettete le vostre modifiche rispettando esattamente questa sintassi:

   ```
   dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
   changetype: modify
   replace: telephoneNumber
   telephoneNumber: +39 1234 567-10
   ```

Leggete la pagina di manuale di ldapmodify (1) per avere delle informazioni dettagliate su `ldapmodify` e la sua sintassi.

29.4.3 Come cercare e leggere dei dati della directory LDAP

OpenLDAP offre con `ldapsearch` un tool a riga di comando per rilevare e leggere dei dati nella directory LDAP. Un comando di ricerca semplice presenta la seguente sintassi:

```
ldapsearch -x -b dc=suse,dc=de "(objectClass=*)"
```

L'opzione `-b` definisce la base di ricerca, cioé il settore dell'albero della directory in cui eseguire la ricerca. Nel nostro esempio `dc=suse,dc=de`. Se volete eseguire una ricerca più mirata in alcuni sottosettori della directory LDAP (p.es. solo nella unità di organizzazione `devel`), consegnate questo settore tramite `-b` a `ldapsearch`. `-x` stabilisce l' utilizzo dell' autenticazione semplice. Con `(objectClass=*)` stabilite che devono essere letti tutti gli oggetti contenuti nella directory. Utilizzate questo comando dopo aver generato un nuovo albero di directory per vedere se le vostre registrazioni sono state assunte correttamente e se il server risponde nel modo desiderato. Per ulteriori informazioni su `ldapsearch` rimandiamo alla relativa pagina di manuale ldapsearch (1).

29.4.4 Cancellare dati da una directory LDAP

Potete cancellare delle registrazioni avvalendovi di `ldapdelete`. La sintassi è simile ai comandi descritti sopra. Per cancellare ad esempio completamente la registrazione `Tux Linux` immettete il seguente comando:

```
ldapdelete -x -D  "cn=admin,dc=suse,dc=de" -W cn=Tux \
Linux,ou=devel,dc=suse,dc=de
```

29.5 Il client LDAP YaST

YaST vi consente di amministrare gli utenti tramite LDAP. Per realizzare ciò, se non è stato già impostato in fase di installazione, invocate il modulo 'Servizi di rete' → 'Client LDAP'. YaST installerà e configurerà automaticamente le modifiche LDAP descritte di seguito per PAM e NSS.

29.5.1 Procedura standard

Per comprendere meglio il funzionamento del modulo client LDAP di YaST dovreste conoscere un po' i processi che si svolgono 'dietro le quinte' sul client. Innazitutto, non appena abilitate durante l'installazione LDAP per l'autenticazione di rete oppure lanciate il modulo YaST, vengono installati i pacchetti `pam_ldap` ed `nss_ldap`, nonché adattati i corrispondenti file di configurazione. Con `pam_ldap` viene utilizzato il modulo PAM preposto alla comunicazione tra processi di login e directory LDAP quale fonte dei dati di autenticazione. Viene installato il relativo modulo `pam_ldap.so` e adattata la configurazione PAM (si veda l'esempio 29.11 in questa pagina).

Esempio 29.11: *pam_unix2.conf adattato per LDAP*

```
auth:       use_ldap nullok
account:    use_ldap
password:   use_ldap nullok
session:    none
```

Se volete configurare manualmente ulteriori servizi LDAP, il modulo LDAP-PAM deve essere inserito nel file di configurazione PAM corrispondente al servizio che trovate sotto `/etc/pam.d/`. File di configurazione già adattati per i singoli servizi si trovano sotto `/usr/share/doc/packages/pam_ldap/pam.d/`. Copiate i file corrispondenti sotto `/etc/pam.d/`.

Tramite `nss_ldap` adattate la risoluzione dei nomi di `glibc`, per via del meccanismo `nsswitch`, all'utilizzo di LDAP. Dopo aver installato questo pacchetto sotto `/etc/` troverete un nuovo file adattato `nsswitch.conf`. Per sapere di più sul funzionamento di `nsswitch.conf` andate alla sezione 22.5.1 a pagina 429. Per l'amministrazione degli utenti ovvero l'autenticazione tramite LDAP, il vostro `nsswitch.conf` deve contenere le seguenti righe (si veda l'esempio 29.12 in questa pagina):

Esempio 29.12: *Adattamenti in nsswitch.conf*

```
passwd: compat
group:  compat

passwd_compat: ldap
group_compat: ldap
```

Queste righe istruiscono la libreria resolver di `glibc`, ad analizzare, quale fonte per i dati di autenticazione e dati utenti, innanzitutto i file corrispondenti locali del sistema sotto `/etc` e di accedere inoltre al server LDAP. Testate questo meccanismo facendovi mostrare tramite il comando `getent passwd` il contenuto della banca dati degli utenti. Nell'elenco dovrebbero comparire sia gli utenti locali del vostro sistema che tutti gli utenti del server LDAP.

Se non volete che sia consentito agli utenti amministrati tramite LDAP di eseguire il login sul server tramite `ssh` o `login` dovete aggiungere un rigo a `/etc/passwd` e `/etc/group` un rigo.

Nel caso di `/etc/passwd` si ha `+::::::/sbin/nologin` e per `/etc/group` `+:::` .

29.5.2 Configurazione del client LDAP

Dopo che `nss_ldap` e `pam_ldap` sono stati adattati da YaST potete iniziare nella prima finestra di YaST con la configurazione vera e propria.

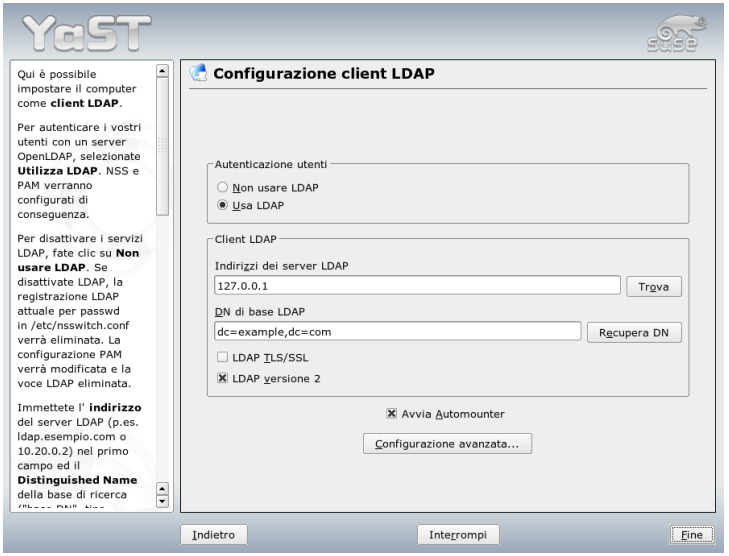

Figura 29.2: *YaST : configurazione del client LDAP*

Nella prima finestra abilitate attraverso radio bottone l'utilizzo di LDAP per l'autenticazione degli utenti e sotto 'DN di base LDAP' immettete la base di ricerca sul server, al di sotto della quale si trovano tutti i dati sul server LDAP. Nel secondo campo di immissione 'Indirizzo dei server LDAP' immettete l'indirizzo del server LDAP. Se volete montare directory remote nel vostro file system abilitate la check box 'Avvia automounter'. Se come amministratore volete modificare dei dati sul server, fate clic su 'Configurazione avanzata' (si veda la figura 29.3 in questa pagina)

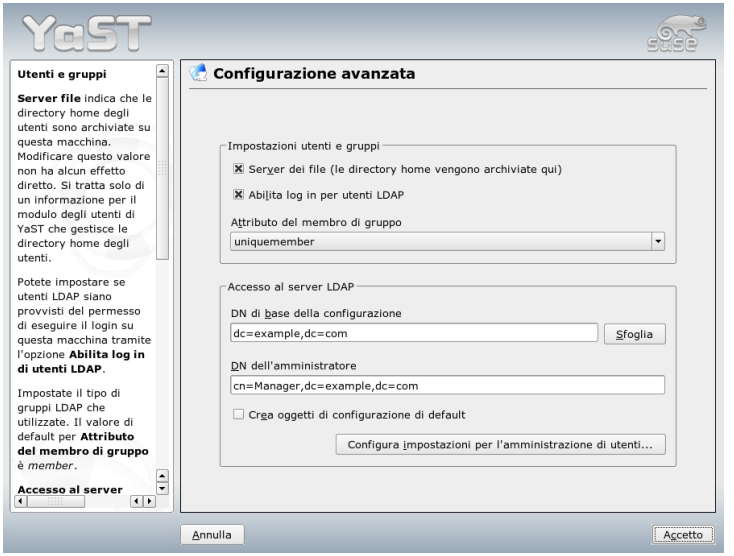

Figura 29.3: *YaST: configurazione avanzata*

Il prossimo dialogo è suddiviso in due parti: nella parte superiore potete eseguire delle impostazioni generali riguardanti utenti e gruppi. Nella parte inferiore inserite i dati di accesso per il server LDAP. Le impostazioni riguardanti utenti e gruppi si limitano alle seguenti voci:

File server Il sistema funge da file server e amministra le directory `/home` degli utenti? Attivando la check box, si assicura che il modulo di YaST gestisce le directory degli utenti in modo appropriato.

Permettere agli utenti LDAP di effettuare il login
Abilitate questa check box per consentire agli utenti amministrati tramite LDAP di effettuare il login sul sistema.

Attributo per il membro del gruppo Determinate il tipo di gruppi LDAP da utilizzare. Avete la scelta tra: 'member' (impostazione di default) e 'uniquemember'.

Per modificare la configurazione del server LDAP immettete in questa finestra i dati di accesso richiesti. Si tratta dei 'DN di base della configurazione', al di sotto dei quali si trovano tutti gli oggetti di configurazione, e 'DN dell' amministratore'.

Per intervenire sulle registrazioni del server LDAP, fate clic su 'Configura le impostazioni per l'amministrazione degli utenti'. Compare una finestra in cui immettere la password LDAP per autenticarsi sul server. In base alle ACL o ACI del server vi sarà concesso l'accesso ai moduli di configurazione sul server.

Importante

Utilizzare client YaST

Il modulo di YaST client LDAP viene utilizzato per adattare ed eventualmente estendere i moduli dell'amministrazione di utenti e gruppi. Inoltre avete la possibilità di definire dei template con dei valori di default per i singoli attributi per semplificare il rilevamento dei dati. I valori qui impostati vengono archiviati nella directory LDAP sotto forma di oggetti LDAP. I dati utenti vanno inseriti tramite il modulo apposito di YaST. Le informazioni vengono archiviate sotto forma di oggetti nella directory LDAP.

Importante

Nel dialogo per la configurazione del modulo (si veda la figura 29.4 nella pagina successiva) avete la possibilità di selezionare e modificare moduli di configurazione esistenti, crearne dei nuovi o creare e modificare dei template per questi moduli. Per modificare il valore all'interno di un modulo di configurazione o per cambiar nome ad un modulo, selezionate il tipo di modulo tramite il combo box sopra la rassegna del contenuto del modulo attuale. Nella rassegna vi è solo un elenco tabellare degli attributi consentiti in questo modulo e dei valori allocati. Qui trovate accanto agli attributi impostati anche altri attributi permessi per via dello schema utilizzato ma attualmente non utilizzati.

Se intendete copiare il modulo, modificate semplicemente `cn`. Per modificare i singoli valori degli attributi, selezionateli nella rassegna dei contenuti e cliccate

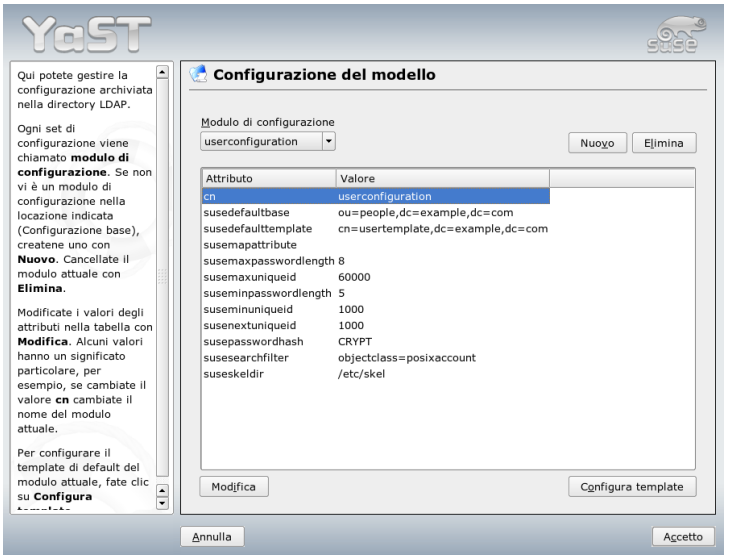

Figura 29.4: *YaST: configurazione del modulo*

su 'Modifica'. Si apre una finestra dialogo dove potete modificare le impostazioni dell'attributo. Con 'OK' rendete effettive le vostre modifiche.

Se volete aggiungere ai moduli uno nuovo, fate clic su 'Nuovo' al di sopra della rassegna dei contenuti. Nel dialogo che appare immettete la classe di oggetto del nuovo modulo (nel nostro caso `suseuserconfiguration` o `susegroupconfiguration`) ed il nome del nuovo modulo. Se uscite dal dialogo con 'OK', il nuovo modulo viene inserito nella lista di selezione dei moduli esistenti e potrà essere selezionato e deselezionato tramite il combo box. Se volete cancellare il modulo attualmente selezionato, fate clic su 'Elimina'.

I moduli YaST per l'amministrazione di gruppi ed utenti integrano template con valori di default sensati se li avete definiti in precedenza tramite il client LDAP di YaST. Per editare dei template fate clic su 'Configura template'. Verranno visualizzati nel menu a tendina template già esistenti che possono essere modificati o una registrazione vuota che vi porta comunque alla maschera per editare i template. Selezionatene uno ed impostate le caratteristiche del template nel seguente dialogo 'Configurazione template dell'oggetto'. Questo dialogo si compone di due finestre con sommari tabellari (si veda la figura 29.5 nella pagina seguente).

Nella finestra superiore sono elencati gli attributi di template generali. Stabilitene valori secondo il vostro scenario di impiego oppure lasciatene dei vuoti. Attributi "vuoti" vengono cancellati sul server LDAP.

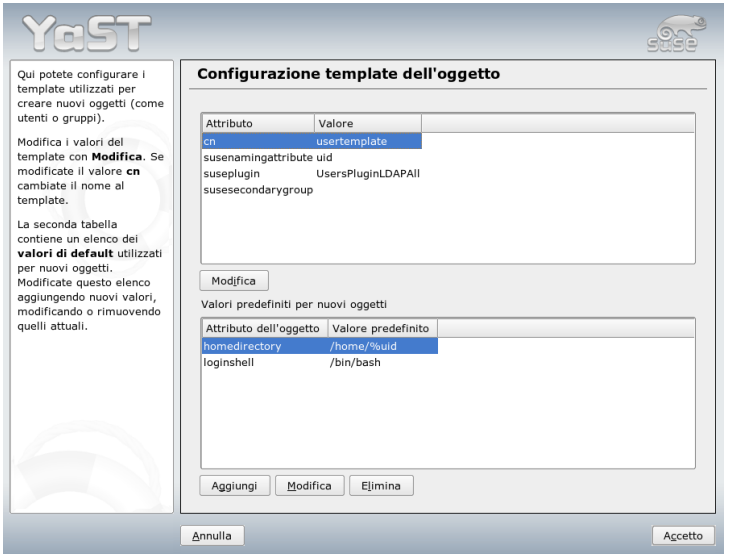

Figura 29.5: *YaST: configurazione di un template di oggetto*

Sotto ('Valori predefiniti per nuovi oggetti') vedete gli attributi del relativo oggetto LDAP (qui: configurazione dei gruppi e utenti), per i quali definite un valore di default. Potete aggiungere ulteriori attributi con valori di default, modificare coppie di attributi - valore e cancellare attributi interi. In egual maniera potete copiare un template modificando la registrazione `cn` per creare un nuovo template. Collegate il template con il relativo modulo impostando come descritto sopra il valore di attributo `susedefaulttemplate` del modulo sul DN del template adattato.

Suggerimento

Potete generare dei valori di default per un attributo da altri attributi utilizzando delle variabili al posto di valori assoluti. Esempio: `cn=%sn %givenName` verrà generato automaticamente dai valori di attributo di `sn` e `givenName`.

Suggerimento

Una volta configurati correttamente i moduli ed i template, con potete creare nuovi gruppi ed utenti.

29.5.3 Utenti e gruppi– configurazione con YaST

Dopo aver configurato i moduli e template per la rete, vi accorgerete che il rilevamento dei dati degli utenti e dei gruppi si discosta solo minimamente dalla procedura da seguire senza l'utilizzo di LDAP. Illustreremo di seguito brevemente l'amministrazione degli utenti, la procedura di amministrazione dei gruppi è analoga.

Il modulo di amministrazione degli utenti di YaST si trova sotto 'Sicurezza & Utenti' → 'Modificare e creare utenti'. Se volete aggiungere un nuovo utente, fate clic su 'Aggiungi'. Si apre una maschera dove potete immettere i principali dati dell'utente come il nome, login e password. Dopo aver inserito i dati premendo il bottone 'Dettagli' potrete configurare in modo più mirato l'appartenenza al gruppo, shell di login e directory home. I valori di default per i campi di immissione sono stati stabiliti in base alla procedura descritta nella sezione 29.5.2 a pagina 512. Se avete abilitato l' uso di LDAP si apre una seconda maschera per l'immissione degli attributi di LDAP (si veda la figura 29.6 nella pagina seguente). Selezionate gli attributi di cui intendete modificare i relativi valori e cliccate su 'Modifica' per aprire la finestra di immissione relativa. Con 'Prossimo' uscite dalla maschera e ritornate alla maschera iniziale per l'amministrazione degli utenti.

Dalla maschera iniziale per l'amministrazione degli utenti il bottone 'Opzioni per esperti' vi dà la possibilità di applicare un filtro di ricerca LDAP agli utenti presenti o di configurare gli utenti e gruppi LDAP di tramite 'Configurazione client e gruppi LDAP'.

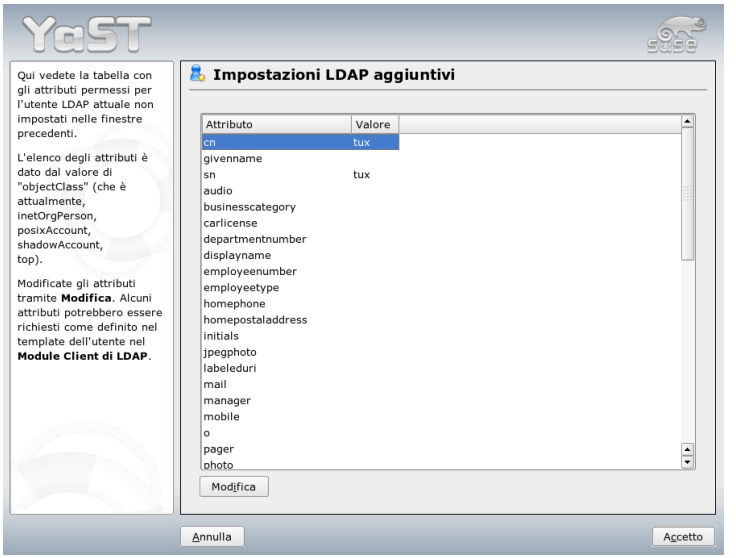

Figura 29.6: *YaST: impostazioni LDAP aggiuntive*

29.6 Ulteriori informazioni

Temi più complessi come la configurazione SASL o l'impostazione di un server LDAP replicante, che si divide il lavoro con "slaves" sono stati esclusi da questo capitolo. Per avere delle informazioni dettagliate su questi temi consultate l'*OpenLDAP 2.2 Administrator's Guide* (per i link si veda sotto).

Sul sito web del progetto OpenLDAP trovate della documentazione dettagliata per utenti LDAP principianti ed esperti:

OpenLDAP Faq-O-Matic Le FAQ in tema di installazione, configurazione ed utilizzo di OpenLDAP: `http://www.openldap.org/faq/data/cache/1.html`

Quick Start Guide Una breve guida per configurare un proprio server LDAP: `http://www.openldap.org/doc/admin22/quickstart.html` o a sistema installato reperibile sotto `/usr/share/doc/packages/openldap2/admin-guide/quickstart.html`

OpenLDAP 2.2 Administrator's Guide
Una introduzione dettagliata per tutti i principali ambiti della configurazione LDAP incl. il controllo degli accessi e cifratura: `http://www.openldap.org/doc/admin22/` o a sistema installato sotto `/usr/share/doc/packages/openldap2/admin-guide/quickstart.html`

Inoltre vi sono i seguenti Redbooks della IBM dedicati al tema LDAP:

Understanding LDAP Una introduzione dettagliata e generale ai principi di base di LDAP: `http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf`

LDAP Implementation Cookbook Si rivolge in particolar modo agli amministratori di *IBM SecureWay Directory*. Vi trovate anche importanti informazioni generali su LDAP: `http://www.redbooks.ibm.com/redbooks/pdfs/sg245110.pdf`

Manuali in inglese su LDAP:

- Howes, Smith & Good: *Understanding and Deploying LDAP Directory Services*. Addison-Wesley, 2. Edizione., 2003. - (ISBN 0-672-32316-8)
- Hodges: *LDAP System Administration*. O'Reilly & Associates, 2003. - (ISBN 1-56592-491-6)

Chiaramente da non dimenticare in tema di LDAP i relativi RFC (ingl. Request for comments) 2251- 2256.

Il server web Apache

Con una quota di mercato di oltre il 60 % (fonte `http://www.netcraft.com`) Apache è il server web più diffuso al mondo. Spesso Apache viene utilizzato a fianco di Linux, del database MySQL e dei linguaggi di programmazione PHP e Perl per la messa a punto di applicazioni web. Per tale combinazione è stata forgiata l'abbreviazione*LAMP*.

In questo capitolo tratteremo il server web Apache. Oltre a indicazioni riguardanti l'installazione e la configurazione descriveremo alcuni moduli. Verranno trattate brevemente anche le varianti per host virtuali.

30.1 I concetti fondamentali

In questa sezione tratteremo le nozioni alla base di un server web e dei protocolli utilizzati in questo campo. Inoltre illustreremo le caratteristiche di primo piano di un server web.

30.1.1 Server web

Il server web fornisce su richiesta pagine HTML ad un client. Queste pagine possono trovarsi in una directory del server (cosiddette pagine passive o statiche) oppure venire generate in risposta ad una richiesta (contenuti attivi).

30.1.2 HTTP

Spesso i client sono dei browser web come Konqueror o Mozilla. Il browser e il server web comunicano tramite l'HTTP, ossia HyperText Transfer Protocol. La documentazione relativa all'attuale versione di HTTP, la 1.1, è reperibile nell' RFC 2068 così come nell'RFC update 2616. Gli RFC sono li trovate al seguente indirizzo URL: `http://www.w3.org`

30.1.3 Le URL

Tramite una URL, il client richiede una pagina a un server. Un esempio: `http://www.suse.de/index.html` Una URL è composta da:

Protocollo I protocolli di maggior diffusione:

- **http://** Il protocollo HTTP.
- **https://** La versione sicura e cifrata di HTTP.
- **ftp://** File Transfer Protocol, per il download e l'upload di file.

Dominio Un dominio, prendiamo il caso di `www.suse.com`. Il dominio è composto da due parti, la prima (`www`) rimanda ad un computer, e la seconda (`suse.com`) che rappresenta il dominio vero e proprio. La prima e la seconda parte compongono insieme il Fully Qualified Domain Name (spesso abbreviato con FQDN) che in italiano potremmo chiamare: nome di dominio completo.

Risorsa Una risorsa, facciamo l'esempio di `index_us.html`. Questa sezione indica il percorso completo della risorsa. Una risorsa può essere un file, come nel nostro esempio, oppure uno script CGI, una Java server page etc.

L'inoltro della richiesta rivolta al dominio `www.suse.com` viene realizzato dai relativi meccanismi dell' Internet (p.es.Domain Name System, DNS), che inoltrano la richiesta di accesso al dominio ad uno o più sistemi di competenza. Apache fornisce poi la risorsa, nel nostro caso si tratta semplicemente della pagina `index.html` presa dalla sua directory dei file. In questo caso il file si trova nella directory principale, ma potrebbe trovarsi anche in una sottodirectory, ad esempio `http://www.support.novell.com/linux/`

Il percorso del file viene specificato nella cosiddetta `DocumentRoot` che può essere modificato nei file di configurazione, come descritto nella sezione DocumentRoot a pagina 529.

30.1.4 Visualizzazione automatica della pagina di default

Quando non vi è alcuna indicazione per la pagina, Apache aggiunge automaticamente all'URL una indicazione molto diffusa per le pagine. `index.html` è l'indicazione più diffusa in questo contesto. Chiaramente potrete impostare questo automatismo che viene descritto nella sezione DirectoryIndex a pagina 530. Nel nostro esempio, immettendo `http://www.suse.com/` il server fornirà la pagina `http://www.novell.com/linux/suse/`.

30.2 Configurare il server HTTP con

Apache può essere configurato in modo veloce e semplice con YaST. Comunque doveste disporre delle nozioni di base se intendete impostare un server web. Se nel centro di controllo di YaST andate su 'Servizi di rete' → 'Server HTTP', eventualmente vi sarà chiesto se installare dei pacchetti mancanti. Non appena avete installato quanto richiesto, giungete alla finestra di configurazione.('Configurazione server HTTP')

Abilitate qui il 'Servizio HTTP', contemporaneamente le porte richieste vengono aperte nel firewall, in questo caso la porta 80 ('Apri firewall sulle porte selezionate'). Nella parte inferiore della finestra ('Impostazioni/Sommario') potete eseguire delle impostazioni per il proprio/i propri server HTTP: 'Ascolta su' (Di default si ha `Porta 80`), 'Moduli', 'Host di default' e 'Hosts'. Tramite 'Modifica' potete intervenire sulle impostazioni relative alla voce selezionata.

Verificate innanzitutto l''Host di default' e adattate eventualmente la configurazione alle vostre esigenze. Attivate quindi tramite 'Moduli' i moduli richiesti. Per configurare dei dettagli vi sono delle ulteriori finestre in particolar modo per l'impostazione di host virtuali.

30.3 Moduli Apache

Tramite dei moduli potete integrare in Apache numerose funzionalità, anche per eseguire degli script CGI nei vari linguaggi di programmazione. E questo non vale solamente per Perl e PHP, ma anche per ulteriori linguaggi di scripting come Python oppure Ruby. Inoltre, vi sono dei moduli per una trasmissione sicura dei dati (secure sockets layer, SSL), l'autenticazione degli utenti, logging esteso e tanto altro ancora.

Potrete compilare dei moduli per adattare Apache anche alle vostre preferenze più insolite. Chiaramente questo presuppone un certo know-how. Per ulteriori informazioni si veda la sezione 30.12.4 a pagina 545

Per l'elaborazione di richieste, Apache utilizza uno o più "handler" (indicati tramite delle direttive nel file di configurazione). Questi handler possono essere parte integrante di Apache oppure un modulo invocato per l'elaborazione della richiesta. In tal modo è data una certa flessibilità nel modo di procedere. Inoltre vi è la possibilità di integrare in Apache dei moduli che avete compilato voi per poter intervenire sul processo di elaborazione delle richieste.

In Apache il concetto di modularizzazione è stato esteso notevolmente: quasi tutto, fatta eccezione per determinati task, viene realizzato tramite dei moduli. Per fare un esempio, in Apache persino il processo di elaborazione di HTTP viene realizzato tramite dei moduli. Apache quindi non deve girare a tutti i costi come server web, grazie ai moduli può assumere anche delle funzioni del tutto differenti. Per esempio vi è un modulo per implementare un server di posta "proof-of-concept" (POP3) basato su Apache.

Apache offre una serie di utili feature, di cui segue una breve rassegna:

Host virtuali Tramite host virtuali con una istanza di Apache su di un singolo sistema potrete gestire diversi siti web, laddove questo procedimento è trasparente per l'utente finale, il quale non si accorge di trovarsi di fronte a un server che gestisce diversi siti web. Gli host virtuali possono essere configurati con diversi indirizzi IP oppure sulla base di nomi. L'hosting virtuale consente di realizzare dei risparmi sul fronte dei costi d'acquisto e su quello del tempo da investire per l'amministrazione di ulteriori sistemi.

Riscrittura flessibile delle URL Apache offre una serie di possibilità per la riscrittura delle URL (URL rewriting). Per ulteriori dettagli consultate la documentazione di Apache.

Content Negotiation Apache, in base alle funzionalità del client (browser), è in grado di fornire delle pagine su misura per il client in questione. In tal modo ad esempio a browser di vecchia data o browser che supportano solo il modo testo (p.es. Lynx) viene fornita una versione semplificata delle pagine, senza frame. In questo modo si aggira il problema derivante all'incompatibilità tra diversi browser in tema di JavaScript, fornendo ad ogni browser una versione adatta delle pagine (se non volete imbarcarvi nell'impresa di adattare il codice JavaScript per ogni singolo browser).

Gestione flessibile di errori Se si verifica un errore (p.es. la pagina non è disponibile) vi è la possibilità di reagire in modo flessibile rispondendo in modo adeguato. Tramite CGI p. es., potrete generare una risposta in modo dinamico.

30.4 Cos'è un thread?

Si tratta di un processo per così dire leggero. Il vantaggio è che un thread necessita di meno risorse rispetto ad un processo, con dei risvolti positivi in termini di performance complessiva. La pecca è che le applicazioni devono essere thread-safe per poter essere eseguite in un ambiente thread, ovvero:

- Le funzioni (o i metodi per applicazioni orientati agli oggetti) devono essere "reentrant", ovvero con lo stesso input devono produrre sempre lo stesso risultato anche se sono diversi thread ad eseguirle contemporaneamente. Le funzioni devono essere quindi programmate in modo da poter essere invocate contemporaneamente da più thread.
- L'accesso alle risorse (spesso delle variabili) deve essere regolato in modo che si non verificano delle interferenze tra thread in esecuzione contemporaneamente.

Apache 2 esegue le richieste sotto forma di processi oppure in forma ibrida composta da processi e thread. L'esecuzione come processo viene realizzato dall'MPM *prefork*, l'esecuzione come thread dall'MPM *worker*. Durante l'installazione potete selezionare (si veda la sezione 30.5 nella pagina seguente) l'MPM da utilizzare. Lo sviluppo del terzo modo, *perchild*, non è ancora del tutto concluso, per tale ragione non è (ancora) disponibile su SUSE LINUX in fase di installazione.

30.5 Installazione

30.5.1 Scelta dei pacchetti in YaST

Per scenari meno complessi basta installare il pacchetto `apache2`. Inoltre va installato uno dei pacchetti MPM (Multiprocessing Module: il `apache2-prefork` oppure il `apache2-worker`. Nella scelta dell'MPM dovete considerare che l'MPM worker non può essere utilizzato assieme al pacchetto `mod_php4`, dato che non tutte le librerie di questo pacchetto sono "threadsafe".

30.5.2 Abilitare Apache

Apache non viene avviato automaticamente dopo esser stato installato. Per lanciare Apache bisogna abilitarlo nell'editor dei runlevel. Per lanciare Apache ad ogni avvio del sistema bisogna inserire un segno di spunta nell'editor dei runlevel per i runlevel 3 e 5. Per vedere se Apache è in esecuzione immettete in un browser l'URL `http://localhost/`. Se Apache è in esecuzione vedrete una pagina esempio, sempre se il pacchetto `apache2-example-pages` è stato installato.

30.5.3 Moduli per contenuti dinamici

Per poter utilizzare dei contenuti dinamici tramite dei moduli bisogna installare i moduli per il relativo linguaggio di programmazione: il pacchetto `apache2-mod_perl` per Perl, il pacchetto `apache2-mod_php4` per PHP ed infine il pacchetto `apache2-mod_python` per Python. Come utilizzare questi moduli viene illustrato nella sezione 30.8.4 a pagina 535.

30.5.4 Altri pacchetti utili

Inoltre è consigliabile installare la documentazione che trovate nel pacchetto `apache2-doc`. Dopo aver installato questo pacchetto e attivato il server (si veda la sezione 30.5.2 in questa pagina) potete invocare la documentazione direttamente tramite l'URL `http.//localhost/manual`.

Coloro che intendono sviluppare dei moduli per Apache oppure compilare dei moduli di terzi devono inoltre installare il pacchetto `apache2-devel` come anche i relativi strumenti di sviluppo, tra cui gli strumenti `apxs` che vengono descritti più dettagliatamente nella sezione 30.5.5 nella pagina successiva.

30.5.5 Installare dei moduli con apxs

Uno strumento di sicuro interesse per sviluppatori di moduli è `apxs2`. Questo programma consente di compilare ed installare (con tutte le modifiche necessarie da apportare ai file di configurazione) tramite un solo comando moduli presenti sotto forma di sorgenti. Inoltre potrete installare dei moduli presenti sotto forma di file oggetto (estensione `.o`) oppure librerie statiche (estensione `.a`). Dai sorgenti, `apxs2` crea un DSO (Dynamic Shared Object) che Apache potrà utilizzare direttamente come modulo.

Con il seguente comando installate un modulo dal file sorgente: `apxs -c -i -a mod_foo.c`. Le altre opzioni di `apxs2` sono descritte nella relativa pagina di manuale. I moduli vanno abilitati tramite la registrazione `APACHE_MODULES` in `/etc/sysconfig/apache2`, come descritto nella sezione 30.6.1 in questa pagina.

Vi sono diverse versioni di `apxs2`: `apxs2`, `apxs2-prefork` e `apxs2-worker`. `apxs2` installa un modulo in modo che sia utilizzabile per tutti gli MPM, gli altri due programmi installano i moduli in modo che possono essere utilizzati solo dal relativo MPM (dunque prefork o rispettivamente worker). Mentre con `apxs2` un modulo viene installato sotto `>/usr/lib/apache2`, nel caso di `apxs2-prefork` il modulo lo si ritroverà sotto `/usr/lib/apache2-prefork`.

30.6 Configurazione

Dopo aver installato Apache dovete intervenire sulla configurazione solo se avete delle esigenze o preferenze particolari. Apache si lascia configurare tramite YaST e SuSEconfig oppure editando direttamente il file `/etc/apache2/httpd.conf`.

30.6.1 Configurazione con SuSEconfig

Le impostazioni che potete effettuare sotto `/etc/sysconfig/apache2`, vengono scritte da SuSEconfig nei file di configurazione di Apache. Le opzioni di configurazione dovrebbero essere sufficienti per la maggior parte dei casi. Ogni variabile è accompagnata da commenti che ne spiegano il significato.

File di configurazione propri

Invece di modificare direttamente il file di configurazione `/etc/apache2/httpd.conf`, la variabile `APACHE_CONF_INCLUDE_FILES` permette di indicare

un file di configurazione proprio (per esempio `httpd.conf.local`, che verrà letto dal file di configurazione principale. In questo modo le vostre modifiche apportate alla configurazione rimangono valide anche se il file `/etc/apache2/httpd.conf` viene sovrascritto durante una reinstallazione.

Moduli

I moduli installati tramite YaST si abilitano immettendo il nome del modulo nella lista sotto la variabile `APACHE_MODULES`. Questa variabile la trovate nel file `/etc/sysconfig/apache2`.

Flags

Con `APACHE_SERVER_FLAGS` potete impostare dei cosiddetti flag che abilitano o disabilitano determinate sezioni del file di configurazione. Per esempio, la sezione del file di configurazione incluso tra

```
<IfDefine someflag>
.
.
.
</IfDefine>
```

viene abilitata solo se presso la variabile `ACTIVE_SERVER_FLAGS` è stato impostato il rispettivo flag: `ACTIVE_SERVER_FLAGS = ... someflag ...` In questo modo potrete eseguire dei test abilitando o disabilitando delle sezioni del file di configurazione.

30.6.2 Configurazione manuale

Il file di configurazione

Il file di configurazione `/etc/apache2/httpd.conf` consente di apportare delle modifiche impossibili da realizzare tramite le impostazioni in `/etc/sysconfig/apache2`. Segue una serie di parametri impostabili nel suddetto file di configurazione. La sequenza in cui vengono riportati i parametri corrisponde in linea di massima a quella del file.

DocumentRoot

Una delle impostazioni principali è la cosiddetta `DocumentRoot`, si tratta della directory che contiene le pagine web che Apache fornirà quando riceve una richiesta. E' impostata su `/srv/www/htdocs` per il host virtuale di default e di solito non è necessario apportare delle modifiche.

Timeout

Indica il tempo che il server fa trascorrere prima di comunicare un timeout (tempo massimo) per una richiesta.

MaxClients

Il numero massimo di client che Apache gestisce contemporaneamente. Il valore di default è `150`, ma per un sito che registra tante richieste potrebbe non essere sufficiente.

LoadModule

Le direttive `LoadModule` indicano i moduli da caricare. Nella versione 2 di Apache la sequenza di caricamento viene stabilita dai moduli. Inoltre, le direttive indicano i file contenenti moduli.

Port

Indica la porta su cui Apache attende delle richieste. Di solito si tratta della porta 80, la porta standard per HTTP. In linea di massima non è consigliato modificare questa impostazione. Un motivo per farlo potrebbe essere quello di voler sottoporre a test una nuova versione aggiornata del sito web. In questo modo la versione del sito in funzione rimane raggiungibile tramite la porta standard 80.

Un altro motivo potrebbe essere quello di voler rendere disponibili delle pagine solo sull' Intranet, perché contengono delle informazioni riservate. In questo caso si imposta la porta sul valore `8080` e si bloccano tutti gli accessi provenienti dall'esterno diretti a questa porta tramite un firewall, in modo che non sia possibile accedere a questo server dall' esterno.

Directory

Tramite questa direttiva vengono impostati i diritti di accesso ed altri diritti concernenti una directory. Anche per la `DocumentRoot` esiste una tale direttiva, il nome di directory lì indicato deve essere modificato sempre ad ogni modifica di `DocumentRoot`.

DirectoryIndex

Qui potete impostare i file da includere nelle ricerche di Apache per completare una URL senza indicazione del file. Il valore di default è `index.html`. Se per esempio un client richiede l'URL `http://www.esempio.com/foo/bar` e sotto la DocumentRoot vi è una directory `foo/bar` che contiene il file `index.html`, Apache ritornerà questa pagina al client.

AllowOverride

Ogni directory da cui Apache fornisce dei documenti può contenere un file atto a modificare i permessi di accesso impostati globalmente ed altre impostazioni che interessano la directory in questione. Queste impostazioni sono ricorsive, cioé valgono per la directory attuale e le sue sottodirectory, finché non vi sia un altro file del genere in una delle sottodirectory. Questo comporta che se impostazioni del genere risiedono in un file che si trova in `DocumentRoot`, allora esse avranno validità globale. Questi file di solito hanno il nome `.htaccess`, che potrete comunque cambiare, si veda a riguardo la sezione AccessFileName nella pagina successiva.

Con `AllowOverride` si stabilisce se le impostazioni indicate nei file locali possano avere la precedenza rispetto alle impostazioni globali. I valori possibili sono `None`, `All` e ogni possibile combinazione tra `Options`, `FileInfo`, `AuthConfig` e `Limit`. Il significato di questi valori viene descritto in modo dettagliato nella documentazione relativa ad Apache. L'impostazione di default (sicura) è `None`.

Order

Questa opzione determina la sequenza nella quale vengono applicate le impostazioni per i permessi di accesso `Allow` e `Deny`, di default si ha:

```
Order allow,deny
```

Quindi per prima cosa vengono applicati i permessi di accesso per accessi consentiti ed in seguito quelli per i permessi negati. Gli approcci sono due:

allow all consentire ogni accesso e definire le eccezioni

deny all negare ogni accesso e definire le eccezioni.

Un esempio per `deny all`:

```
Order deny,allow
Deny from all
Allow from example.com
Allow from 10.1.0.0/255.255.0.0
```

AccessFileName

Qui potete impostare il nome per i file che non devono attenersi alle impostazioni globali riguardanti i permessi di accesso ed altre impostazioni delle directory fornite da Apache (si veda anche la sezione AllowOverride a fronte). Di default si ha `.htaccess`.

ErrorLog

Indica il nome del file con i messaggi di errore di Apache. Di default si tratta del file `/var/log/httpd/errorlog`. Anche i messaggi di errore per host virtuali (si veda la sezione 30.9 a pagina 539) si trovano in questo file se nella sezione `VirtualHost` del file di configurazione non è stato indicato un altro file di log.

LogLevel

I messaggi di errore sono suddivisi - in base alla gravità - in diversi livelli. Qui potete impostare a partire da quale livello di gravità protocollare il messaggio. Verranno protocollati i messaggi del livello impostato e quelli dei livelli superiori in termini di gravità. Il valore di default è `warn`.

Alias

Tramite un alias potete indicare una abbreviazione per accedere direttamente ad una determinata directory. Per fare un esempio: tramite l'alias `/manual/` potrete accedere direttamente alla directory `/srv/www/htdocs/manual`, anche nel caso in cui la DocumentRoot è impostata su una directory diversa da `/srv/www/htdocs` (non si ha alcuna differenza con l'alias, se la `DocumentRoot` è impostata su questa directory.) Nel caso di questo alias con `http://localhost/manual` si accede direttamente alla directory relativa. Per avere dei permessi per la nuova directory meta in base a quanto specificato nella direttiva `Alias` dovrete eventualmente specificare una direttiva `Directory` per la directory in questione (si veda a riguardo sezione Directory a pagina 529).

ScriptAlias

Questa direttiva è simile a quella `Alias` indicando inoltre che i file nella directory meta debbano essere trattati come script CGI.

Server Side Includes (SSI)

I cosiddetti Server Side Include abbreviati con SSI possono essere abilitati ricercandoli negli eseguibili con il comando

```
<IfModule mod_include.c>
XBitHack on </IfModule>
```

Per eseguire una ricerca degli SSI in un file, basta renderlo eseguibile con `chmod +x`⟨*nomefile*⟩; oppure si può indicare in modo esplicito il tipo di file in cui ricercare gli SSI, che si realizza con

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

Non è consigliabile indicare qui semplicemente `.html`, dato che Apache effettuerà una ricerca degli SSI in tutte le pagine (anche in quelle che per motivi di sicurezza non contengono degli SSI), cosa che ha dei risvolti negativi dal punto di vista della performance. In SUSE LINUX queste due istruzioni sono già contenute nel file di configurazione, dunque normalmente non sarà necessario apportare degli adattamenti.

UserDir

Con il modulo `mod_userdir` e la direttiva `UserDir` si indica una directory nella directory home dell' utente con i file da pubblicare su Internet tramite Apache. Ciò viene impostato in SuSEconfig tramite la variabile `HTTPD_SEC_PUBLIC_HTML`. Per pubblicare dei file, la variabile va impostata sul valore `yes`. Nel file `/etc/apache2/mod_userdir.conf` (che viene letto da `/etc/apache2/httpd.conf`) si avrà una registrazione del tipo:

```
<IfModule mod_userdir.c>
UserDir public_html
</IfModule>
```

30.7 Apache in azione

Per visualizzare con Apache proprie pagine web (statiche), basta collocare i propri file nella directory giusta. Nel caso di SUSE LINUX si tratta di `/srv/www/`

`htdocs`. Può darsi che vi sono già installate delle piccole pagine esempio che servono solo per vedere se Apache sia stato installato correttamente e giri nel modo dovuto; queste pagine possono essere sovrascritte o eliminate. I vostri script CGI li potete installare sotto `/srv/www/cgi-bin`.

In esecuzione Apache scrive i propri messaggi di log nel file `/var/log/httpd/access_log` o `/var/log/apache2/access_log`. Nel file di log viene documentata l'ora ed il metodo (`GET`, `POST`...) con ill quale sono state richieste e messe a disposizione le risorse. In caso di errore trovate le indicazioni attinenti nel file `/var/log/apache2`.

30.8 Contenuti dinamici

Apache offre una serie di possibilità per fornire ad un client dei contenuti dinamici. Per contenuti dinamici si intendono pagine HTML create in base ai dati di input variabili del client. Un esempio noto sono i motori di ricerca che dopo aver immesso uno o più termini, eventualmente collegati tramite degli operatori logici come "AND" oppure "OR',' ritornano un elenco di pagine che contengono il termine o i termini indicati.

Con Apache vi sono tre modi per creare dei contenuti dinamici:

Server Side Includes (SSI) Si tratta di direttive embedded nelle pagine HTML tramite dei commenti particolari. Apache analizza il contenuto dei commenti e emette il risultato quale parte della pagina HTML.

Common Gateway Interface (CGI) In questo caso vengono eseguiti dei programmi che risiedono in determinate directory. Apache consegna a questi programmi i parametri trasmessi dal client, e ritorna l'output del programma Questo modo di programmare è relativamente semplice, anche perché i programmi a linea di comando esistenti possono essere modificati in modo da accettera dell'input di Apache e ritornare l'output ad Apache.

Moduli Apache offre delle interfacce per poter eseguire dei moduli come parte del processo di elaborazione della richiesta, ed inoltre consente a questi programmi di accedere ad informazioni importanti, tipo request o intestazioni HTTP. Ciò rende possibile integrare dei programmi nel processo di elaborazione che non sono solo in grado di creare dei contenuti dinamici ma anche di assumere altre funzioni (p.es. autenticazione). Programmare questo tipo di moduli richiede una certa abilità; i vantaggi che ne conseguono sono alte prestazioni e possibilità che vanno ben oltre a quanto offerto dagli SSI e CGI.

Mentre gli script CGI vengono eseguiti da Apache (con l'ID dell'utente del loro proprietario), per i moduli viene utilizzato un interprete embedded in Apache che sotto l'ID del server web è permanentemente in esecuzione, per tal ragione si usa l'espressione interprete "persistente". In questo modo non deve venire inizializzato e terminato un proprio processo per ogni richiesta (cosa che crea un overhead considerevole per l'amministrazione dei processi, della memoria etc.), ma è l'interprete già in esecuzione con l'ID del server web a gestire lo script.

Lo svantaggio comunque è rappresentato dal fatto che mentre gli script eseguiti tramite CGI sono abbastanza tolleranti nei riguardi di errori di programmazione, questa caratteristica non è data quando si ricorre ai moduli. Il motivo è dovuto alla circostanza che i comuni errori negli script CGI, come il non liberare risorse e memoria, non comportano delle particolari conseguenze, visto che dopo l'elaborazione della richiesta questi programmi vengono terminati e lo spazio di memoria negato in precedenza dal programma, a causa di un errore di programmazione, è nuovamente disponibile. Quando si utilizzano invece dei moduli gli effetti degli errori di programmazione si accumulano, dato che l'interprete è permanentemente in esecuzione. Se non si riavvia il server, l'interprete girerà per mesi interi, e così con il tempo si faranno sentire gli effetti di richieste negate di liberare delle risorse.

30.8.1 Server Side Includes:SSI

Server Side Includes sono delle direttive embedded in commenti particolari eseguiti da Apache. Il risultato viene integrato subito nell'output. Un esempio: potete farvi indicare la data attuale con `<!--#echo var="DATE_LOCAL" -->`; laddove # indica l'inizio del commento e `<!--` è l' indicazione per Apache, che si tratta di una direttiva SSI e non di un solito commento.

Gli SSI possono essere abilitati in modi diversi. La variante più semplice consiste nell' eseguire una ricerca dei SSI nei file eseguibili. L'altra possibilità consiste nello stabilire il tipo di file nei quali cercare gli SSI. Entrambi gli approcci vengono illustrati nella sezione Server Side Includes (SSI) a pagina 532.

30.8.2 Common Gateway Interface:CGI

CGI è l'abbreviazione di *Common Gateway Interface*. Tramite la CGI il server non fornisce semplicemente una pagina HTML statica, ma esegue un programma che genera la pagina. In questo modo possono venir create delle pagine che sono il risultato di un calcolo, per esempio il risultato di una ricerca in una banca dati. Al

programma che viene eseguito si possono consegnare degli argomenti in modo che ritorni una pagina su misura per ogni richiesta.

Il vantaggio della CGI sta nella sua semplicità. Il programma deve solo risiedere in una determinata directory, e il server web lo eseguirà proprio alla stregua di un programma la riga di comando. Il server inoltra l'output del programma sul canale standard di emissione (`stdout`) al client.

In linea di massima i programmi CGI possono essere scritti in ogni linguaggio di programmazione. Di solito vengono utilizzati a tale scopo dei linguaggi di scripting (linguaggi interpretati) come Perl oppure PHP; se si pone l'accento sulla velocità si propone C oppure C++.

Apache si aspetta questi programmi in una determinata directory (`cgi-bin`). Questa directory si lascia impostare nel file di configurazione, si veda la sezione 30.6 a pagina 527. Inoltre si possono stabilire ulteriori directory in cui Apache debba eseguire le sue ricerche di programmi eseguibili. Questo comporta un certo rischio in termini di sicurezza, visto che ogni utente potrà far eseguire da Apache dei programmi (possibilmente nocivi). Se invece i programmi eseguibili sono consentiti solo in `cgi-bin`, l'amministratore potrà verificare più facilmente chi vi archivia quali script e programmi, ed eventualmente verificare se si tratta di file che possono arrecare danno.

30.8.3 GET e POST

I parametri di immissione possono essere consegnati al server con `GET` oppure con `POST`. Il metodo utilizzato determina il modo in cui il server consegna i parametri allo script. Nel caso di `POST` il server passa i parametri al programma tramite il canale standard di input (`stdin`) proprio come se il programma venisse avviato in una console. Nel caso di `GET` il server consegna i parametri al programma tramite la variabile di ambiente `QUERY_STRING`.

30.8.4 Creare contenuti dinamici tramite moduli

Vi sono una serie di moduli per Apache. Il termine "modulo" viene utilizzato con due accezioni: da una parte vi sono moduli che possono essere integrati in Apache e assumere una determinata funzione, come ad esempio i moduli che presenteremo di seguito, i quali integrano i linguaggi di programmazione in Apache.

Dall'altra, in ambito dei linguaggi di programmazione, si parla di moduli per indicare una serie di funzionalità, classi e variabili. Questi moduli vengono integrati in un programma per offrire una determinata funzionalità. Un esempio è rappresentato dai moduli CGI presenti in tutti i linguaggi di programmazione che facilitano la programmazione di applicazioni CGI mettendo a disposizione dei metodi per leggere dei parametri di request e per l'output HTML.

30.8.5 mod_perl

Perl è un linguaggio di scripting molto diffuso e collaudato. Vi è una vastità di moduli e librerie per Perl (tra l'altro anche una libreria per estendere il file di configurazione di Apache). La home page di Perl è `http://www.perl.com/`. Nel Comprehensive Perl Archive Network (CPAN) troverete una serie di librerie per Perl `http://www.cpan.org/`.

Configurare mod_perl

Per configurare `mod_perl` in SUSE LINUX basta installare il relativo pacchetto (si veda la sezione 30.5 a pagina 526). Le registrazioni necessarie per Apache sono già incluse nel file di configurazione, si veda `/etc/apache2/mod\_perl-startup.pl`. Per raccogliere delle informazioni su `mod_perl` visitate il seguente sito:`http://perl.apache.org/`

mod_perl vs. CGI

Gli script CGI possono essere lanciati come script `mod_perl` invocandoli attraverso un'URL diversa. Il file di configurazione contiene degli alias che rimandano alla stessa directory, e che lanciano gli script ivi contenuti tramite CGI oppure tramite `mod_perl`. Tutte le registrazioni sono già presenti nel file di configurazione. L'alias per CGI è:

```
ScriptAlias /cgi-bin/ "/srv/www/cgi-bin/"
```

Le registrazioni per `mod_perl` sono:

```
<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>
```

Servono anche le seguenti registrazioni per `mod_perl` che comunque sono già presenti nel file di configurazione.

```
#
# 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>
```

Queste registrazioni creano gli alias per i modi `Apache::Registry` e `Apache::PerlRun`. Ecco in cosa differiscono:

Apache::Registry Tutti gli script vengono compilati e tenuti nella cache. Ogni script viene generato come contenuto di una subroutine. Anche se questo produce degli effetti positivi dal punto di vista della performance, lo svantaggio è che gli script devono essere programmati in modo impeccabile visto che le variabili e le subroutine permangono anche tra chiamate diverse. Bisogna resettare le variabili affinché possano essere utilizzate nuovamente alla prossima chiamata. Se per esempio il codice della carta di credito di un cliente viene salvato in una variabile di uno script per l'online banking, potrebbe accadere che il codice ricompaia quando è un altro cliente ad utilizzare l'applicazione ed a richiedere lo stesso script.

Apache::PerlRun Gli script vengono ricompilati ad ogni nuova richiesta, in modo che le variabili e le subroutine scompaiono dal name space tra una

chiamata e l'altra. Il name space è l'insieme dei nomi delle variabili e dei nomi di routine definito in un dato momento dall'esistenza di un determinato script. Dunque con `Apache::PerlRun` non bisogna porre particolare attenzione ad una programmazione senza sbavature, dato che le variabili all'avvio dello script vengono inizializzate ex novo e quindi non possono contenere dei valori risalenti a chiamate precedenti. Questo va però a discapito della velocità, ma è comunque più veloce di CGI (nonstante delle somiglianze con CGI), visto che non bisogna lanciare un processo per l'interprete.

30.8.6 mod_php4

PHP è un linguaggio di programmazione ideato appositamente per server web. A differenza di altri linguaggi i cui i comandi si trovano in determinati file detti script, i comandi di PHP (similmente agli SSI) si trovano embedded ovvero contenuti in una pagine HTML. L'interprete PHP processa i comandi PHP ed integra il risultato dell'elaborazione nella pagina HTML.

La home page di PHP è `http://www.php.net/`. Il pacchetto `mod_php4-core` va installato in ogni caso, per Apache 2 va installato inoltre il pacchetto `apache2-mod_php4`.

30.8.7 mod_python

Python è un linguaggio di programmazione orientato agli oggetti con una sintassi chiara e ben leggibile. Una particolarità di questo linguaggio è che la struttura del programma dipende dall'indentazione. I singoli blocchi non vengono definiti da parentesi graffe o simili (come in C e Perl) oppure da indicazioni `begin` e `end`, è il grado di indentazione a svolgere questo ruolo. Installate il pacchetto `apache2-mod_python`.

Per saperne di più, visitate il sito `http://www.python.org/`. Per maggior informazioni su `mod_python` visitate il sito `http://www.modpython.org/`.

30.8.8 mod_ruby

Ruby è un linguaggio di programmazione di alto livello orientato agli oggetti relativamente recente che presenta delle similitudini sia con Perl che con Python, e che si adatta benissimo per script. La sintassi chiara e ben strutturata ricorda

Phyton, mentre coloro che apprezzano Perl gradiranno (gli altri meno) la presenza delle abbreviazioni tipici di Perl. In termini di concetto di base Ruby ricorda Smaltalk.

La home page di Ruby: `http://www.ruby-lang.org/`. Anche per Ruby vi è un modulo Apache, ecco la home page: `http://www.modruby.net/`.

30.9 Host virtuali

Grazie agli host virtuali è possibile gestire più domini con un solo server web. In tal modo è possibile risparmiare sul fronte dei costi e lavoro manutenzione necessario se si ha un server dedicato per ogni dominio. Vi sono diversi modi per realizzare l'hosting virtuale:

- Hosting virtuale basato su nome
- Hosting virtuale basato sull'IP
- Eseguire diverse istanze di Apache su una macchina.

30.9.1 Hosting virtuale basato su nome

In questo caso una istanza di Apache gestisce diversi domini. Non è richiesta l'impostazione di diversi indirizzi IP per un sistema. Si tratta della alternativa che presenta le minori difficoltà, ed è quindi da preferire. Consultate la documentazione di Apache per sapere di più sui possibili svantaggi dell'hosting virtuale basato su nome.

La configurazione si realizza direttamente tramite il file di configurazione `/etc/apache2/httpd.conf`. L'hosting virtuale basato su nome si abilita tramite una direttiva: `NameVirtualHost *`. Basta indicare `*`, per fare accettare ad Apache tutte le richieste in entrata. In seguito si devono configurare i singoli host virtuali:

```
<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>
```

Una registrazione `VirtualHost` va configurata per il dominio ospitato sul server (`www.example.com`). Nel nostro esempio, lo stesso server ospita accanto al domino originario un secondo dominio (`www.myothercompany.com`).

Anche le direttive `VirtualHost`, come nel caso di `NameVirtualHost`, hanno un *. Apache mappa la richiesta all'host virtuale in base al campo host nell'intestazione HTTP. La richiesta viene fatta pervenire all' host virtuale il cui `ServerName` corrisponde al nome host indicato in tal campo.

Per quel che riguarda le direttive `ErrorLog` e `CustomLog` i file di log non devono necessariamente contenere il nome di dominio, si possono utilizzare dei nomi a caso.

`ServeraAdmin` indica l'indirizzo e-mail dell' amministratore a cui rivolgersi in caso di difficoltà. Se si verificano degli errori Apache indicherà questo indirizzo nella comunicazione di errore inviata ai client.

30.9.2 Hosting virtuale basato sull'IP

In questo caso bisogna impostare diversi indirizzi IP per una macchina. Una istanza di Apache amministrerà diversi domini, laddove ogni dominio disporrà di un indirizzo IP. Nel seguente esempio illustreremo come configurare Apache in modo da ospitare oltre al suo indirizzo IP originario (`192.168.1.10`) anche due domini con due ulteriori indirizzi IP (`192.168.1.20` e `192.168.1.21`). Questo esempio concreto funziona solo in una Intranet, dato che gli indirizzi IP tra `192.168.0.0` e `192.168.255.0` non vengono instradati su Internet.

Impostare l'aliasing degli IP

Affinché Apache possa ospitare diversi indirizzi IP, il sistema su cui gira deve accettare delle richieste per indirizzi IP diversi. In questi casi si parla di multi-IP hosting; per realizzare ciò si deve innanzitutto abilitare l'aliasing di indirizzi IP nel kernel, cosa che in SUSE LINUX è già impostato di default.

Se il kernel è stato configurato per consentire l'aliasing di indirizzi IP, tramite i comandi `ifconfig` e `route` si possono impostare ulteriori indirizzi IP. Per poter

immettere questi comandi bisogna entrare nel sistema come `root`. Nel seguente esempio partiamo dal presupposto che il sistema abbia già un proprio indirizzo IP, ad esempio `192.168.1.10`, assegnato al dispositivo di rete `eth0`.

L'IP della macchina si lascia visualizzare immettendo `ifconfig`. Ulteriori indirizzi IP si aggiungono ad esempio con

```
ip addr add 192.168.1.20/24 dev eth0
```

Gli indirizzi IP vanno assegnati ad un dispositivo di rete fisico (`eth0`).

Host virtuali con IP

Dopo aver configurato l'aliasing di indirizzi IP o dopo aver installato diverse schede di rete, si può proseguire con la configurazione di Apache. Per ogni server virtuale si indica un proprio blocco `VirtualHost`:

```
<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>
```

Qui si indicano le direttive `VirtualHost` per ulteriori domini, il dominio originario (`www.example.com`) viene configurato attraverso le proprio impostazioni (sotto `DocumentRoot` etc.) all'infuori dei blocchi `VirtualHost`.

30.9.3 Più istanze di Apache

Nei metodi fin qui descritti gli amministratori di un dominio possono leggere i dati degli altri domini. Se si vogliono isolare i singoli domini, si possono lanciare più istanze di Apache con impostazioni proprie per `User`, `Group` ed altre direttive nel file di configurazione.

Nel file di configurazione con la direttiva `Listen` si indica quale istanza di Apache è responsabile per quale indirizzo IP. Per la prima istanza di Apache, riprendendo l'esempio di prima, la direttiva sarà:

```
Listen 192.168.1.10:80
```

Per le altre due istanze rispettivamente:

```
Listen 192.168.1.20:80
Listen 192.168.1.21:80
```

30.10 Sicurezza

30.10.1 Ridurre i rischi

Se non vi serve un server web, disabilitate Apache nell' editor dei runlevel oppure non installatelo proprio. Meno funzionalità server sono abilitati, meno si è esposti ad eventuali attacchi. Questo vale in particolar modo per sistemi che fungono da firewall, sui quali per principio non dovrebbe girare alcun server.

30.10.2 Permessi di accesso

root, il proprietario di DocumentRoot

Di default `root` è il proprietario della directory `DocumentRoot` (`/srv/www/htdocs`) e della directory CGI. Cosa che non dovrebbe essere modificata, altrimenti chiunque con accesso in scrittura a queste directory potrebbe archiviarvi dei file che verrebbero eseguiti da Apache come utente `wwwrun`. Apache non dovrebbe avere dei permessi di scrittura per file e script che consegna, quindi il proprietario di questi file e script non dovrebbe essere `wwwrun`, ma ad esempio `root`.

Se si desidera dare agli utenti la possibilità di deporre dei file nella directory documento di Apache, invece di concedere l'accesso in scrittura a tutti, è preferibile creare una sottodirectory con accesso in scrittura per tutti, ad esempio `/srv/www/htdocs/sottodir`.

Pubblicare dei documenti dalla propria directory home

Un altro modo per dare agli utenti la possibilità di pubblicare dei propri file su Internet è di indicare nel file di configurazione una directory nella directory home dell'utente in cui l'utente può deporrvi i suoi file per presentazioni web (p.es. `~/public_html`). In SUSE LINUX questa funzionalità è abilitata di default, per ulteriori dettagli rimandiamo alla sezione UserDir a pagina 532.

A queste pagine web si potrà accedere indicando l'utente nella URL; l'URL avrà una indicazione `~nomeutente` quale abbreviazione per la relativa directory nella directory home dell'utente. Esempio: immettendo l' URL `http://localhost/~tux` in un browser verranno visualizzati i file della directory `public_html` nella directory home dell'utente tux.

30.10.3 Essere sempre aggiornati

Chi amministra un server web, soprattutto se si tratta di un server web di dominio pubblico, dovrebbe essere sempre aggiornato soprattutto in tema di bug e dei rischi che ne conseguono in termini di sicurezza. Nella sezione 30.12.3 nella pagina successiva sono elencate le fonti per documentarsi su exploit e bug-fix.

30.11 Come risolvere possibili problemi

Cosa fare quando vi sono delle difficoltà, per esempio se Apache non visualizza una pagina o la visualizza non correttamente? Come prima cosa consultate i file error-log, per vedere se dai messaggi si riesce ad individuare la causa del disturbo: `/var/log/apache2/error_log` è il file di log principale.

Una altra possibilità consiste nel visualizzare i file di per vedere in tempo reale il modo di reagire del server alle richieste. Se volete farlo, basta immettere in una console `root` il seguente comando:

```
tail -f /var/log/apache2/*_log
```

Date una occhiata al bug database che trovate sotto `http://bugs.apache.org/` Tenetevi informati tramite mailing list e newsgroup. La mailing list per utenti la trovate sotto `http://httpd.apache.org/userslist.html`; quale newsgroup consigliamo `comp.infosystems.www.servers.unix` e simili.

Se gli approcci illustrati finora non portano al risultato desiderato e siete sicuri di trovarvi di fronte ad un baco di Apache, rivolgetevi direttamente a `http://www.suse.de/feedback/`.

30.12 Ulteriore documentazione

Apache è un server web molto diffuso, quindi è reperibile tanta documentazione su diversi siti web che vi potrà essere di aiuto e di supporto.

30.12.1 Apache

Anche Apache dispone di una documentazione esaustiva, come installarla sul vostro sistema viene descritto nella sezione 30.5 a pagina 526. La troverete in seguito sotto `http://localhost/manual`. La documentazione aggiornata chiaramente la troverete sempre sulla home page di Apache: `http://httpd.apache.org`

30.12.2 CGI

Per avere ulteriori informazioni sulla CGI visitate i seguenti siti:

- `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 Sicurezza

Sotto `http://www.novell.com/linux/security/securitysupport.html` trovate sempre le patch attuali per pacchetti SUSE LINUX da poter scaricare. Visitate regolarmente questa URL, qui potrete anche abbonarvi tramite mailing list di SUSE “Security Announcements”.

ll team di Apache sostiene una politica di informazione trasparente per quanto riguarda l’esistenza di errori in Apache. Le ultime notizie su bug e parti del sistema esposti a degli attacchi le trovate all’indirizzo: `http://httpd.`

apache.org/security_report.html. Se avete scoperto una falla nella sicurezza di Apache (siete pregati di verificare prima nelle fonti sopra indicate se si tratta davvero di un problema non già rilevato), potete rivolgervi via e-mail a security@suse.de o anche a security@apache.org.

Altri fonti di informazioni in tema di sicurezza per Apache (ed altre applicazioni web):

- http://www.cert.org/
- http://www.vnunet.com/
- http://www.securityfocus.com/

30.12.4 Ulteriori fonti

Nel caso incontraste delle difficoltà, vale la pena consultare la banca dati di supporto della SuSE (in inglese): http://portal.suse.com/sdb/en/index.html. Una rivista online su Apache la trovate sotto: http://www.apacheweek.com/

Le origini di Apache vengono descritte sotto http://httpd.apache.org/ABOUT_APACHE.html. Qui scoprirete anche perché il server porta il nome Apache.

Per informarvi in tema di upgrade dalla versione 1.3 alla 2.0 rimandiamo a http://httpd.apache.org/docs-2.0/en/upgrading.html.

Sincronizzazione dei file

Oggi sono in tanti a utilizzare ed a lavorare con più di un computer. Spesso se ne ha uno a casa, uno o più di uno al lavoro ed eventualmente anche un portatile o PDA che si utilizza durante gli spostamenti. Molti file dovranno essere disponibili su tutti quanti i computer con i quali si lavora per poterli elaborare, e chiaramente tutti i dati dovranno essere disponibili nella versione aggiornata su ogni sistema.

31.1 Software per la sincronizzazione dei dati

Nel caso di computer che compongono i singoli nodi di una rete veloce, la sincronizzazione dei dati non rappresenta un problema. Basta selezionare un file system di rete, per esempio NFS e salvare i file su un server. I vari computer accederanno in seguito tramite la rete agli stessi e identici dati depositati sul server. Questo approccio diventa improponibile nel caso di una rete molto lenta o nel caso di connessione saltuaria. Chi usa un laptop durante i suoi spostamenti necessità delle copie dei file da elaborare sul proprio disco rigido locale. Non appena però si inizia a modificare i file si presenta il problema della sincronizzazione. Se si modifica un file su un computer si deve badare assolutamente ad aggiornare la copia del file su tutti gli altri computer. Se si tratta di un fatto sporadico questo si lascia realizzare comodamente a mano con i comandi scp o rsync. Nel caso di numerosi file il tutto diventa già un po' più laborioso e richiede molta attenzione per evitare che si sovrascriva ad esempio un file nuovo con la vecchia versione.

Avvertimento

Occhio alla perdita di dati

In ogni caso bisogna sapere usare bene il programma impiegato e testare le sue funzionalità prima di amministrare i propri dati tramite un sistema di sincronizzazione. La copia di sicurezza è ed resta irrinunciabile per file importanti.

Avvertimento

Per risparmiarsi queste procedure laboriose che richiedono tanto tempo prezioso e sono esposte ad errori vi è del software che seguendo approcci diversi automatizza questo processo. La seguente breve introduzione intende solamente dare all'utente un'idea del modo di funzionare di questi programmi e di come adoperarli. Prima di utilizzarli effettivamente consigliamo di leggere attentamente la documentazione relativa.

31.1.1 Unison

Unison non è un file system di rete. I file vengono editati e salvati in locale. Si può richiamare il programma manualmente per sincronizzare i file. La prima volta che si esegue il processo di sincronizzazione viene creata una banca

dati su entrambi i sistemi coinvolti nella quale vengono memorizzate le somme di controllo, la data ed i permessi dei file selezionati. Alla prossima chiamata, unison è in grado di riconoscere i file che hanno subito delle modifiche e ne propone la trasmissione da un sistema all'altro. Solitamente potrete accettare tranquillamente le proposte di unison.

31.1.2 CVS

Impiegato soprattutto per l'amministrazione di varie versioni di sorgenti di programmi, CVS consente di avere delle copie dei file su diversi computer. In questo senso è adatto anche al nostro scopo. Il CVS ha un database centrale chiamato repository, che risiede sul server, ed il quale memorizza non solo i file ma anche le singole modifiche apportate ai file. Quando le modifiche eseguite in locale vengono immesse nel database, si parla di commit, le quali potranno essere scaricate dagli altri computer (update). Entrambi i processi vengono eseguiti dall'utente.

Inoltre CVS è tollerante nei confronti di errori riguardanti le modifiche effettuate da diversi computer: le modifiche vengono raccolte e solo se vi sono delle modifiche che interessano la stessa riga di un documento o file sorge un conflitto. Il database, in caso di un conflitto, resta comunque in uno stato consistente; il conflitto è visibile solo sul client e solamente da lì risolvibile.

31.1.3 subversion

Al contrario di CVS che è "cresciuto" con il tempo, nel caso di subversion ci troviamo di fronte ad un progetto portato avanti sin dal principio in modo consistente. subversion è stato concepito per sostituirsi a CVS.

subversion presenta una serie di migliorie rispetto al suo predecessore. CVS è in grado di amministrare solo file e "ignora" le directory. subversion invece offre uno storico anche per le directory che potranno essere copiate e rinominate alla stregua di file. Inoltre, è possibile aggiungere per ogni file e directory dei metadati relativi ad una determinata versione del file o directory. A differenza di CVS, subversion consente un accesso di rete transparente grazie a dei propri protocolli come ad esempio WebDAV (Web-based Distributed Authoring and Versioning) che estende le funzionalità del protocollo HTTP fino a permettere accessi simultanei in scrittura su file residenti su server web remoti.

subversion è stato realizzato in prima linea ricorrendo a pacchetti di applicazioni già esistenti. Infatti subversion utilizza il server web Apache e l'estensione WebDAV.

31.1.4 mailsync

A differenza dei tool di sincronizzazione finora menzionati, Mailsync sincronizza solo e-mail di caselle diverse. Si può trattare sia di e-mail nella mail box locale che di mail box che risiedono su un server IMAP.

Per ogni messaggio viene deciso sulla base del message id, contenuto nell'intestazione della e-mail, se cancellarlo o sincronizzarlo. E' possibile sincronizzare sia singole mail box che gerarchie di mail box.

31.1.5 rsync

Se non vi occorre un'applicazione che vi permetta di controllare le singole versioni ed intendete sincronizzare vasti alberi di file tramite connessioni di rete lente, allora potete ricorrere al tool rsync. rsync dispone di meccanismi particolari che consentono di trasmettere solo le modifiche apportate ai file, siano essi file di testo oppure dei binari. Per rilevare le differenze tra i file, rsync suddivide i file in blocchi e ne calcola la somma di controllo.

Però il rilevamento delle modifiche ha il suo prezzo. rsync richiede tra l'altro tanta RAM.

31.2 Criteri per scegliere il programma giusto

31.2.1 Client-server vs. peer-to-peer

Per la sincronizzazione dei dati si sono diffusi due modelli. Nel primo caso vi è un server centrale in base al quale i client sincronizzano i loro file. I client dovranno potersi collegare via rete almeno temporaneamente al server. Questo modello è quello utilizzato da subversion, CVS e WebDAV

L'alternativa è rappresentata da computer "equiparati" che sincronizzano i loro dati a vicenda. Questo è l'approccio che segue unison. rsync segue l'approccio client-server, comunque ogni client può fungere a sua volta da server.

31.2.2 Portabilità

Subversion, CVS, e unison sono disponibili per tutta una serie di sistemi operativi tra cui UNIX e Windows.

31.2.3 Interattivo vs. automatico

Con subversion, CVS WebDAV, e unison la sincronizzazione viene inizializzata manualmente dall'utente. Il vantaggio è che si ha maggior controllo sul processo di sincronizzazione ed è più facile risolvere dei conflitti. Dall'altra parte, se la sincronizzazione viene effettuata troppo di rado aumentano le probabilità che si verifichi un conflitto.

31.2.4 Il verificarsi e la risoluzione di conflitti

In subversion o CVS i conflitti si verificano solo raramente anche se sono diverse persone a lavorare ad un grande progetto. I documenti vengono costruiti riga dopo riga. Quando si verifica un conflitto, spesso ciò riguarda solo un client. Generalmente, nel caso di subversion o CVS i conflitti sono semplici da risolvere.

Unison comunica il verificarsi di conflitti e si potranno escludere i file imputati dal processo di sincronizzazione. Tuttavia non è così semplice allineare le modifiche come nel caso di subversion o CVS.

Mentre con subversion o CVS quando si verifica un conflitto, le modifiche possono essere assunte anche parzialmente, nel caso di WebDAV un check-in può essere eseguito solo se il processo di modifica nel suo intero non ha prodotto dei conflitti.

rsync non presenta delle funzionalità per trattare ed eliminare eventuali dei conflitti. L'utente dovrà fare attenzione a non sovrascrivere per errore dei file e risolvere manualmente i conflitti che affioriranno. Per andare sul sicuro, si potrà ricorrere ad applicazioni di versionamento come RCS.

31.2.5 Selezionare e aggiungere dei file

Unison sincronizza interi alberi di directory. I file che si aggiungono all'albero vengono inclusi automaticamente nel processo di sincronizzazione.

In subversion o CVS bisogna aggiungere esplicitamente nuovi file e directory tramite il comando `svn add` o `cvs add`. In tal modo si ha un maggior controllo sui file da sincronizzare. Dall'altra parte spesso si dimenticano i nuovi file, soprattutto se nell'output di `svn update`, `svn status` o `cvs update` si ignorano i '?' (punti interrogativi) a causa della mole dei file.

31.2.6 Lo storico

Subversion o CVS permettono inoltre di ricostruire versioni precedenti di un file. Ad ogni modifica potrete aggiungere un breve commento per poter meglio seguire e rintracciare le varie modifiche apportate al file in passato. Questa funzionalità si rivela di particolare utilità nella stesura di tesi o di sorgenti.

31.2.7 Volume dei dati e spazio sul disco rigido richiesto

Su ogni computer interessato serve spazio a sufficienza per i dati dislocati. Per subversion o cvs serve inoltre dello spazio aggiuntivo per la banca dati (il cosiddetto repository) sul server. Visto che sul server viene memorizzato anche lo storico dei dati è necessario ulteriore spazio. Nel caso di file di testo, il fabbisogno non è eccessivo anche perché vengono memorizzate solo le righe modificate; mentre per file binari ad ogni modifica il fabbisogno cresce nella misura del volume del file.

31.2.8 GUI

Unison dispone di una interfaccia grafica che indica cosa il programma intende sincronizzare. Si può accettare la proposta o escludere singoli file dalla sincronizzazione. Inoltre è possibile confermare in modo interattivo i singoli processi nel modo testo.

Gli utente più esperti impiegano CVS di solito servendosi della riga di comando. Comunque vi sono anche interfacce grafiche per Linux (cervisia…) ed anche per Windows (wincvs). Tanti tool di sviluppo (p.es. kdevelop) ed editor di testo (p.es. emacs) supportano CVS o subversion. Grazie a questi front-end risolvere dei conflitti diventa davvero semplice.

31.2.9 User friedliness

unison e rsync sono semplici da utilizzare ed indicati anche per principianti. CVS o subversion sono già un po' più complessi nel loro utilizzo. Per un eventuale impiego si dovrebbe aver afferrato il modo di interagire tra il repository e i dati in locale. In locale si dovrebbe innazitutto avere comunque la versione aggiornata dei file, questo si ottiene con il comando `cvs update` o `svn update`. Dopo aver eseguito questo comando, con il comando `cvs commit` o `svn commit` i dati vanno rispediti nel repository. Se si segue sempre questa procedura CVS o subversion risultano essere semplici da utilizzare anche per principianti.

31.2.10 Sicurezza contro attacchi

La protezione contro l'intercettazione o addirittura la manipolazione dei dati durante il loro trasferimento dovrebbe essere sempre data. Sia per unison che CVS, rsync o subversion si può ricorrere a ssh (Secure Shell) per mettersi al riparo da eventuali attacchi. Evitate di utilizzare rsh (remote shell) con CVS o unison e anche gli accessi tramite il meccanismo *pserver* del CVS non sono consigliabili in rete non protette. subversion è per questi casi già più indicato, visto che offre i necessari meccanismi di sicurezza tramite l'utilizzo di Apache.

31.2.11 Sicurezza contro la perdita di dati

CVS viene utilizzato da già tempo da tanti sviluppatori per amministrare i propri progetti ed è estremamente stabile. Grazie allo storico, con CVS si è anche al riparo di determinati errori causati da disattenzioni dell'utente (p.es. cancellare per errore un file). Anche se subversion non gode della diffusione di CVS, viene già utilizzato in modo produttivo (si veda l'esempio dello stesso progetto subversion).

Unison è un prodotto relativamente recente ma è già molto stabile. L'utente dovrà fare molta attenzione per evitare degli errori: se ad esempio accetta di cancellare un file durante il processo di sincronizzazione, il file risulterà irrecuperabile.

Tabella 31.1: *Feature dei tool di sincronizzazione -- = molto scarso, - = scarso o non disponibile, o = mediocre, + = buono, ++ = molto buono, x = disponibile*

	unison	**CVS/subv.**	**rsync**	**mailsync**
Client/Server	uguale	C-S/C-S	C-S	uguale
Portabil.	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x
Interattivo	x	x/x	x	-
Velocità	-	o/+	+	+
Conflitti	o	++/++	o	+
Selez. file	Directory	Selez./file,direct.	Directory	Mail box
Storico	-	x/x	-	-
Spazio dis.	o	--	o	+

GUI	+	o/o	-	-
Difficoltà	+	o/o	+	o
Attacchi	+(ssh)	+/+(ssh)	+(ssh)	+(SSL)
Perdita di dati	+	++/++	+	+

31.3 Introduzione ad unison

Unison si adatta perfettamente ai fini della sincronizzazione e del trasferimento di interi alberi di directory. La sincronizzazione avviene in entrambi le direzioni e si lascia gestire facilmente tramite un front-end grafico (alternativamente potete utilizzare anche la versione console). Sussiste anche la possibilità di automatizzare il processo di sincronizzazione, cioé far svolgere il tutto senza che sia richiesto un intervento da parte dell'utente.

31.3.1 Presupposti

Unison deve essere installato sia sul client che sul server; con *server* in questi casi si intende un computer remoto (a differenza di CVS, si veda la sezione 31.1.2 a pagina 549).

Dato che nella seguente esposizione ci limiteremo all'impiego di unison con ssh, dovrà essere installato un client ssh sul client ed un server ssh sul server.

31.3.2 Utilizzo di Unison

Il principio di base di Unison consiste nel collegare due directory (cosiddette*roots*), o meglio collegare in senso simbolico - non si tratta un collegamento online. Facciamo un esempio: ammettiamo di avere il seguente layout di directory:

Client:	`/home/tux/dir1`
Server:	`/home/geeko/dir2`

Volete sincronizzare entrambi le directory. Sul client, l'utente è noto come tux e sul server invece come `geeko`. Innanzitutto si dovrebbe eseguire un test per verificare il corretto funzionamento della comunicazione tra il server e il client:

```
unison -testserver /home/tux/dir1
ssh://geeko@server//homes/geeko/dir2
```

Ecco le principali difficoltà che potrebbero sorgere a questo punto:

- le versioni di unison utilizzate sul client e sul server non sono compatibili
- il server non permette una connessione SSH
- nessuno dei due percorsi indicati esiste

Se tutto funziona come deve, si tralascia l'opzione `-testserver`. Durante la prima sincronizzazione unison non conosce ancora il rapporto che intercorre tra le due directory, e fa delle proposte per quando riguarda la direzione di trasferimento dei singoli file e directory. Le frecce nella colonna 'Azione' indicano la direzione di trasferimento. Il punto interrogativo '?' indica che unison non riesce a fare una proposta riguardo alla direzione di trasferimento, dato che entrambi le versioni nel frattempo sono state modificate o sono nuove.

Con i tasti freccia si può impostare la direzione di trasferimento per ogni singola registrazione. Una volta stabilita la direzione di trasferimento per le registrazioni visualizzate, fate clic semplicemente su 'Vai'.

Unison (ad es. per eseguire automaticamente la sincronizzazione nei casi evidenti) può ricevere all'avvio dei parametri dalla riga di comando. Un elenco completo dei parametri si ottiene con `unison ---help`.

Esempio 31.1: *Il file ~/.unison/example.prefs*

```
root=/home/tux/dir1
root=ssh://wilber@server//homes/wilber/dir2
batch=true
```

Ogni processo di sincronizzazione viene protocollato nella directory dell'utente `~/.unison`. In questa directory si possono immettere anche set di configurazione, per es. `~/.unison/example.prefs`. Per inizializzare la sincronizzazione basta semplicemente indicare il file come argomento della riga di comando: `unison example.prefs`

31.3.3 Ulteriore documentazione

La documentazione ufficiale su unison è davvero esaustiva, nel presente capitolo ci siamo limitati ad una breve introduzione. Sotto `http://www.cis.upenn.edu/~bcpierce/unison/` o nel pacchetto SUSE `unison` troverete un manuale completo.

31.4 Introduzione a CVS

CVS può essere utilizzato anche ai fini della sincronizzazione, quando si modificano frequentemente singoli file nel formato di testo ASCII oppure sorgenti di programmi. Con CVS si possono sincronizzare anche dati in altri formati (p.es. file JPEG), ma questo comporta un enorme volume di dati, visto che ogni variante di un file viene memorizzata permanentemente sul server CVS. Ed inoltre in questi casi non si sfrutta appieno il vero potenziale di CVS. Si consiglia di ricorrere a CVS per la sincronizzazione dei dati solo se tutte le postazioni di lavoro hanno accesso allo stesso server!

31.4.1 Impostare un server CVS

Il *server* è host su cui si trovano tutti i file validi, ovvero soprattutto la versione attuale di ogni file. Una una postazione di lavoro fissa può fungere da server. E' consigliabile eseguire regolarmente un back-up dei dati che risiedono sul server CVS (repository).

Si consiglia di impostare un server CVS in modo che agli utenti sia permesso di accedervi tramite SSH. Se l'utente è noto al server come `tux` ed il software del CVS è stato installato sia sul server che sul client (p.es. un notebook), sul lato client bisogna impostare le seguenti variabili di ambiente:

```
CVS_RSH=ssh CVS_ROOT=tux@server:/serverdir
```

Con il comando `cvs init` si inizializza il server CVS dal lato client (basta farlo una sola volta).

Infine bisogna stabilire un nome per la sincronizzazione. Selezionate o create una directory sul client che dovrà contenere i file che dovranno essere amministrati da CVS (la directory può essere anche vuota). Il nome della directory è nel contempo il nome del processo di sincronizzazione. Nel nostro esempio utilizziamo il nome `synchome`. Per impostare il nome della sincronizzazione su `synchome` si deve immettere:

```
cvs import synchome tux wilber
```

Attenzione: molti comandi CVS richiedono un commento. A tale scopo CVS lancia un editor (più precisamente l'editor definito nella variabile di ambiente `$EDITOR`, altrimenti lancia il vi). Si può evitare che venga lanciato l'editor immettendo il commento già nella riga di comando, ad es

```
cvs import -m 'questa è una prova' synchome tux wilber
```

31.4.2 Utilizzare il CVS

A partire da questo momento si può effettuare da un computer qualsiasi il check out dal repository di sincronizzazione con `cvs co synchome`. Si avrà una nuova sottodirectory `synchome` sul client. Se si sono fatte delle modifiche che si vogliono comunicare al server, bisogna entrare nella directory `synchome` (o anche in una sottodirectory di synchome) ed immettere il seguente comando: `cvs commit`.

Con questo comando vengono trasmessi al server tutti i file della la directory (sottodirectory incluse). Per trasferire solo singoli file e/o singole directory, si dovranno indicare esplicitamente con un comando del tipo: `cvs commit file1 directory1`. Nuovi file o nuove directory vanno aggiunte alla repository tramite un comando del tipo: `cvs add file1 directory1`, prima di trasferirli sul server. Di conseguenza il commit di nuovi file e directory che si sono aggiunti si esegue tramite `cvs commit file1 directory1`.

Se cambiate postazione di lavoro, dovrete, se non lo avete già fatto durante delle sessioni di lavoro precedenti sulla stessa postazione, eseguire il check out del repository (si veda sopra).

La sincronizzazione con il server viene inizializzata con: `cvs update`. Sussiste inoltre la possibilità di eseguire l'update di singoli file e/o singole directory eseguendo `cvs update file1 directory1`. Se volete vedere in anteprima le differenze rispetto alle versioni memorizzate sul server, immettete `cvs diff` o `cvs diff file1 directory1`. In più avete anche la possibilità di farvi mostrare quali file verrebbero aggiornati, ecco il comando: `cvs -nq update`.

Durante l'update incontrerete tra l'altro le seguenti lettere indicanti lo stato del file:

U la versione locale è stata aggiornata.

M la versione locale è stata modificata.

P la versione locale è stata adattata (ingl. patched) in base alla versione sul server.

C il file locale non collima con la versione attuale nel repository.

? questo file non esiste nel CVS.

`M` indica un file che è stato modificato. Potete spedire la versione locale al server o cancellare il file locale e si esegue nuovamente un update. Se diversi utenti modificano lo stesso file nello stesso punto, CVS non è in grado di decidere quale versione utilizzare. In questi casi all'update si ha una `C` che indica la presenza di un conflitto.

In tal caso prendete spunto dai marcatori di conflitto e decidete quale delle due versioni scegliere. Visto che a volte non è per niente semplice prendere una tale decisione, potete anche optare di scartare le vostre modifiche, cancellare il file locale e immettere `cvs up` per recuperare la versione attuale dal server.

31.4.3 Ulteriore documentazione

Le possibilità di impiego di CVS sono immense e noi abbiamo fornito solo una breve introduzione. Per degli approfondimenti rimandiamo alla documentazione reperibile tra l'altro ai seguenti indirizzi:

```
http://www.cvshome.org/
http://www.gnu.org/manual/
```

31.5 Un 'introduzione a subversion

Subversion è un sistema di controllo di versionamento a sorgente aperto che succede a CVS. Le caratteristiche già trattate di CVS si ritrovano generalmente anche in subversion che presenta tutti i vantaggi di CVS senza riproporrne gli svantaggi. Molte delle caratteristiche sono state già trattate nella sezione 31.1.3 a pagina 549.

31.5.1 Configurare un server subversion

Impostare un repository su un server è un processo davvero semplice. subversion dispone di un proprio tool. Per generare un nuovo repository, immettete:

```
svnadmin create /percorso/del/repository
```

Per visualizzare ulteriori opzioni, immettete `svnadmin help`. A differenza di CVS, subversion non si basa su RCS ma su la banca dati Berkeley. *Non* create una repository su file system remoti come NFS, AFS o Windows SMB. La banca dati richiede dei meccanismi di locking POSIX che i file sytem menzionati non offrono.

Per visionare il contenuto di un repository, vi è il comando `svnlook`:

```
svnlook info /percorso/del/repository
```

Affinché anche altri utenti possano accedere al repository va configurato un server; potrà trattarsi di un server web Apache con WebDAV o del server di subversion, svnserve. Se svnserve è in esecuzione si potrà accedere ad una repository tramite L'URL `svn://` o `svn+ssh://`. Tramite il file di configurazione `/etc/svnserve.conf` potete indicare gli utenti che dovranno autenticarsi se invocano `svn`.

Rispondere alla domanda quale sistema di versionamento scegliere non è facile, dato che vanno considerati una serie di fattori. Si consiglia di dare un'occhiata al manuale di subversion (per maggiori informazioni, si veda la sezione 31.5.3 a pagina 561).

31.5.2 Utilizzo

Per accedere ad un repository di subversion vi è il comando `svn` (simile a `cvs`). Se il server è stato configurato in modo corretto (con relativo repository) il contenuto di ogni client può essere visionato con:

```
svn list http://svn.example.com/percorso/del/progetto
```

oppure

```
svn list svn://svn.example.com/percorso/del/progetto
```

Con il comando `svn checkout` un dato progetto può essere salvato nella directory attuale (ingl. check out):

```
svn checkout http://svn./percorso/del/progetto nomeprogetto
```

Il check out crea una nuova sottodirectory `nomeprogetto` sul client, in cui poter eseguire tutta una serie di modiche come aggiungere, copiare, rinominare e cancellare dei file:

```
svn add file
svn copy vecchiofile nuovofile
svn move vecchiofile nuovofile
svn delete file
```

Questi comandi sono applicabili anche a delle directory. Inoltre subversion è in grado di indicare le cosiddette properties, ossia proprietà di un file o di una directory:

```
svn propset license GPL foo.txt
```

Nell'esempio precedente è stato impostato il valore `GPL` per la proprietà `license`. Le proprietà si lasciano visualizzare con `svn proplist`.

```
svn proplist --verbose foo.txt
Properties on 'foo.txt':
  license : GPL
```

Per salvare le modifiche sul server, immettete `svn commit`. Affinché un altro utente possa disporre delle vostre modifiche nella sua directory di lavoro, dovrà eseguire un `svn update`.

A differenza di CVS, lo stato di una directory di lavoro subversion può essere visualizzato anche *senza* accesso al repository con `svn status`. Le modifiche locali vengono visualizzate in cinque colonne, la prima è quella di maggiore rilevanza:

" Nessuna modifica

'A' Oggetto da aggiungere

'D' Oggetto da eliminare

'M' Oggetto modificato

'C' Oggetto in stato di conflitto

'I' Oggetto ignorato

'?' Oggetto non incluso nel controllo di versionamento

'!' Oggetto manca. Questo stato si ha se l'oggetto è stato eliminato o spostato senza ricorrere al comando `svn`.

'~' Oggetto amministrato come file è stato sostituito da una directory o viceversa.

La seconda colonna indica lo stato delle properties. Tutte le altre colonne vengono illustrate nel manuale di subversion.

Se vi dovesse sfuggire il parametro di un comando, provate con, `svn help`:

```
   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 Ulteriore documentazione

Innazitutto vi è la home page del progetto subversion che trovate al seguente indirizzo `http://subversion.tigris.org/`. Se installate il pacchetto `subversion-doc` nella directory `file:///usr/share/doc/packages/subversion/html/book.html` sarà a vostra disposizione un manuale in inglese completo che vale davvero la pena di leggere. Tra l'altro è anche disponibile online sotto `http://svnbook.red-bean.com/svnbook/index.html`.

31.6 Un'introduzione a rsync

rsync si propone ogni qualvolta si debbano trasmettere grandi volumi di dati con cadenze più o meno regolari. Cosa che si ha spesso quando si esegue un back-up,

ovvero una copia di sicurezza. Un ulteriore campo di applicazione è rappresentato dai cosiddetti staging server, ovvero server su cui risiede l'intero albero directory di un server web che viene specchiato con cadenze regolari sull'effettivo server web in una "DMZ".

31.6.1 Configurazione e utilizzo

rsync può essere utilizzato in due modi diversi. rsync può essere utilizzato per archiviare e copiare dei file, a tal fine è richiesta solo una shell remota, come ad esempio ssh, sull'host meta. rsync può però fungere anche da `daemon` e mettere a disposizione delle directory nella rete.

Per utilizzare rsync non è richiesta una configurazione particolare. rsync permette di specchiare direttamente delle intere directory su di un altro host. Ad esempio con il seguente comando è possibile avere un back-up della directory home di tux sul server di back-up sole:

```
rsync -baz -e ssh /home/tux/ tux@sole:backup
```

Per il processo inverso si immette:

```
rsync -az -e ssh tux@sole:backup /home/tux/
```

Fin qui il funzionamento non si distingue particolarmente da una comune applicazione per effettuare delle copie, come scp.

Per sfruttarne a fondo le potenzialità, rsync dovrebbe girare nel modo "rsync". A tal fine va avviato su un host il daemon rsyncd. In questo caso rsync si configura tramite il file `/etc/rsyncd.conf`. Se ad esempio intendete rendere accessibile la directory `/srv/ftp` tramite rsync potete utilizzare il file di configurazione riportato:

```
gid = nobody
uid = nobody
read only = true
use chroot = no
transfer logging = true
log format = %h %o %f %l %b
log file = /var/log/rsyncd.log

[FTP]
        path = /srv/ftp
        comment = Un esempio
```

In seguito si dovrà lanciare rsyncd con `rcrsyncd start` rsyncd può essere lanciato anche automaticamente durante il processo di boot, basta abilitare il servizio nell' editor dei runlevel di YaST oppure immettere manualmente il comando `insserv rsyncd`. Come alternativa rsyncd può essere lanciato anche da xinetd. Ciò si consiglia solo nel caso di server su cui non si utilizza spesso rsyncd.

Nell'esempio di sopra viene creato anche un file di log che protocolla tutte le connessioni, lo ritroverete sotto `/var/log/rsyncd.log`.

A questo punto si potrà seguire il transfer da un client, tramite il comando:

```
rsync -avz sole::FTP
```

Questo comando elenca tutti i file che si trovano sul server nella directory `/srv/ftp`. Questa richiesta riemerge anche nel file di log sotto `/var/log/syncd.log`. Per avviare il transfer va indicata una directory meta. Per indicare la directory attuale potete anche utilizzare un `.`, quindi:

```
rsync -avz sole::FTP .
```

Di default durante il processo di sincronizzazione eseguito tramite rsync non vengono eliminati dei file. Se si vuole forzare tale operazione, basta indicare in aggiunta l'opzione `--delete`. Per garantire che non vengano sovrascritti dei file aggiornati potete indicare l'opzione `--update`. Se dovessero verificarsi dei conflitti, questi dovranno essere risolti manualmente.

31.6.2 Ulteriore documentazione

Le indicazioni di maggior rilevanza su rsync sono contenute nelle pagine di manuale che potete visualizzare con `man rsync` e `man rsyncd.conf`. Per delle indicazioni di natura tecnica su rsync rimandiamo a `/usr/share/doc/packages/rsync/tech_report.ps`. Per delle informazioni aggiornate su rsync visitate il sito web del progetto che trovate sotto `http://rsync.samba.org`.

31.7 Introduzione a mailsync

Mailsync assolve principalmente tre compiti:

- sincronizza e-mail memorizzati in locale con e-mail memorizzati su un server
- esegue la migrazione di mail box in un altro formato o su un altro server
- verifica l'integrità di una mail box o cerca i doppioni

31.7.1 Configurazione ed utilizzo

Mailsync distingue tra mail box in sé (un cosiddetto *store*) e il collegamento tra due mail box (un cosiddetto *channel*). La definizione degli store e dei channel viene archiviata nel file `~/.mailsync`. Seguono alcuni esempi relativi agli store.

Una semplice definizione ha ad es. il seguente aspetto:

```
store saved-messages {
        pat     Mail/saved-messages
        prefix  Mail/
}
```

dove `Mail/` è una sottodirectory nella directory home dell'utente, contente una cartella con le e-mail, tra l'altro la cartella `saved-messages`. Se si invoca mailsync con il comando `mailsync -m saved-messages` in `saved-messages` si avrà un indice con tutti i messaggi. Un altro esempio:

```
store localdir {
          pat     Mail/*
          prefix  Mail/
}
```

In questo caso invocando `mailsync -m localdir` verranno elencati tutti i messaggi salvati sotto `Mail/`. Il comando `mailsync localdir` elenca invece i nomi delle cartelle. La specificazione di uno store sul server IMAP p.es. ha il seguente aspetto:

```
store imapinbox {
  server  {mail.edu.bocconi.it/user=gulliver}
  ref     {mail.edu.bocconi.it}
  pat     INBOX
}
```

Nell'esempio riportato sopra vengono semplicemente indirizzate il folder, ossia cartella principale sul server IMAP. Uno store per le sottocartelle assumerebbe il seguente aspetto:

```
store imapdir {
server {mail.edu.harvard.com/user=gulliver}
ref {mail.edu.harvard.com}
pat INBOX.*
prefix  INBOX.
}
```

Se il server IMAP supporta connessioni cifrate, la specificazione del server dovrebbe essere modificata nel modo seguente:

```
server  {mail.edu.bocconi.it/ssl/user=gulliver}
```

o (se non conoscete il certificato del server) in

```
server {mail.edu.bocconi.it/ssl/novalidate-cert/user=gulliver}
```

Il prefisso viene spiegato in seguito.

Ora le cartelle sotto `Mail/` vanno connesse alle sottodirectory sul server IMAP:

```
channel cartella localdir imapdir {
        msinfo .mailsync.info
}
```

Mailsync utilizza il file `msinfo` per tenere traccia dei messaggi già sincronizzati.

Invocando `mailsync cartella` si ottiene che:

- la mail box venga allineata su entrambi gli host
- il prefisso dai nomi delle cartelle che si creano durante il processo venga eliminato
- le cartelle vengano sincronizzate a due a due (o create se ancora non esistenti)

La cartella `INBOX.sent-mail` sul server IMAP viene quindi sincronizzata con la cartella locale `Mail/sent-mail` (ciò presuppone le definizioni di cui sopra). Infine viene eseguita la sincronizzazione delle singole cartelle nel modo seguente:

- se il messaggio esiste su entrambi gli host, non succede niente
- se il messaggio manca da una parte e si tratta di un messaggio nuovo, cioé non protocollato nel file `msinfo`, viene trasmesso lì dove manca

- se il messaggio esiste solo su una parte e si tratta di un messaggio già vecchio ovvero già protocollato nel file `msinfo`, viene cancellato da lì (dato che il messaggio che esisteva è stato cancellato sull' altro host)

Per avere una vista di insieme a priori dei messaggi che verranno trasmessi e quali cancellati durante la sincronizzazione, bisogna richiamare Mailsync contemporaneamente con un channel *ed* uno store: `mailsync cartella localdir`. In tal maniera si avrà un elenco dei messaggi che sono nuovi sull'host locale ed anche una lista di tutti i messaggi che verrebbero cancellati sul lato server IMAP durante la sincronizzazione. Inversamente con `mailsync cartella imapdir` si ottiene un'elenco dei messaggi nuovi sul lato IMAP ed anche un'elenco dei messaggi che verrebbero cancellati sull'host locale durante la sincronizzazione.

31.7.2 Possibili difficoltà

Nel caso si verifichi una perdita di dati, il modo più sicuro di procedere è quello i cancellare i relativi file di protocollo channel `msinfo`. In tal modo tutti i messaggi che esistono solo da una parte vengono considerati dei nuovi messaggi e verranno trasmessi durante la prossima sincronizzazione.

Saranno presi in considerazione per quanto riguarda la sincronizzazione solo quei messaggi che hanno una cosiddetta message ID. I messaggi sprovvisti di un tale identificativo verranno ignorati, cioé non verranno né trasmessi né cancellati. Spesso la mancanza della message ID è dovuta a errori da ricondurre a dei programmi in fase di invio o creazione delle e-mail.

Su determinati server IMAP la cartella principale viene indirizzata tramite `INBOX`, e le sottocartelle tramite un nome qualsiasi (a differenza di INBOX ed INBOX.name). In tal modo per questi server IMAP non è possibile specificare un campione esclusivamente per le sottocartelle.

I driver per mail box (c-client) utilizzati da Mailsync, una volta trasmessi correttamente i messaggi ad un server IMAP, impostano una speciale indicazione di stato (status flag) per cui alcuni programmi di posta elettronica come mutt non riescono ad riconoscere i nuovi messaggi come tali. Per evitare che ciò avvenga vi è l'opzione `-n`.

31.7.3 Ulteriore documentazione

Nel `README` contenuto nel pacchetto `mailsync` sotto `/usr/share/doc/packages/mailsync/` sono reperibili ulteriori informazioni ed indicazioni. Di particolare interesse in questo contesto è anche l'RFC 2076 "Common Internet Message Headers".

Samba

Con Samba è possibile trasformare un qualsiasi computer Unix in un server di file e stampa per client DOS, Windows ed OS/2: questo capitolo tratta le basi di una configurazione Samba ed illustra i moduli YaST tramite i quali è possibile configurare Samba nella vostra rete.

Samba è ormai diventato un prodotto maturo. In questo capitolo tratteremo brevemente le sue funzionalità di base. Comunque il software viene fornito con documentazione esaustiva in forma digitale. Immettere `apropos samba` sulla riga di comando per visualizzare delle pagine di manuale oppure sotto `/usr/share/doc/packages/samba`, una volta installato Samba sono reperibili una serie di esempio e ulteriore documentazione. Nella sottodirectory `examples` trovate anche la configurazione esempio commentata `smb.conf.SuSE`.

Il pacchetto `samba`, è a vostra disposizione nella 3. versione. Ecco alcune delle principali novità del pacchetto:

- Supporto a Active Directory.
- Perfezionamento del supporto di Unicode.
- Rielaborazione completa dei meccanismi di autenticazione interna.
- Miglior supporto per il sistema di stampa Windows 200x/XP.
- Possibilità di configurare dei server quali membri di domini Active-Directory.
- Assunzione di domini NT4 per poter effettuare la migrazione verso un dominio Samba.

Suggerimento

Migrare verso Samba3

Se intendete migrare da Samba 2.x verso Samba 3 dovete tenere presente alcune particolarità. A questo tema è stato dedicato un intero capitolo nella Samba HOWTO Collection. Dopo aver installato il pacchetto `samba-doc` l' HOWTO è reperibile sotto `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

Suggerimento

Samba utilizza il protocollo SMB (Server Message Block), che si basa sui servizi di NetBIOS. Cedendo alle richieste della IBM, la Microsoft ha reso pubblico il protocollo in modo da permettere anche ad altri fornitori di software di poter collegarsi ad una rete Microsoft. Samba implementa il protocollo SMB su TCP/IP. Così su ogni client deve essere installato il protocollo TCP/IP. Noi consigliamo di utilizzare esclusivamente TCP/IP sui client.

NetBIOS è un'interfaccia software (API) ideata per la comunicazione tra client; si ricorre ad un cosiddetto name service che permette alle macchine connesse in rete di riservarsi un nome, tramite il quale potranno essere indirizzate. Non vi è una istanza centrale ad assegnare i nomi, ogni host nella rete può riservarsi un nome non ancora assegnato. L'interfaccia di NetBIOS può venire implementata su diverse architetture di rete. NetBEUI è un'implementazione che interagisce in modo stretto con l'hardware di rete. NetBEUI viene spesso chiamato NetBIOS. Altri protocolli di rete con cui è stato implementato NetBIOS sono IPX (NetBIOS tramite TCP/IP) di Novell e TCP/IP.

I nomi NetBIOS inviati tramite TCP/IP non hanno niente a che vedere con i nomi utilizzati nel file `/etc/hosts` o assegnati via DNS - NetBIOS dispone di un proprio "name space", ovvero di una propria convenzione per i nomi. Per semplificare l'amministrazione si consiglia tuttavia di dare almeno ai server dei nomi NetBIOS che corrispondano al nome host DNS; per un server Samba ciò avviene di default.

Tutti i comuni sistemi operativi, come Mac OS X, Windows e OS/2 supportano il protocollo SMB. Sul client deve essere installato il protocollo TCP/IP. Samba mette a disposizione anche un client per le diverse versioni di UNIX. Per Linux esiste inoltre un modulo del kernel per SMB che permette di integrare risorse SMB nel sistema Linux.

I server SMB mettono a disposizione dei loro client dello spazio su hard disk sotto forma di cosiddette "share". Una share comprende una directory con tutte le sottodirectory sul server; viene esportata con un nome proprio e può venire indirizzata dai client sotto questo nome. A questo scopo, il nome della share può essere assegnato liberamente. Non può comunque corrispondere al nome della directory esportata. Allo stesso modo viene attribuito un nome ad una stampante esportata, attraverso il quale i client possono indirizzarla.

32.1 Configurazione del server

Se volete utilizzare Samba come server installate il pacchetto `samba`. I servizi necessari a Samba vengono avviati manualmente con il comando `rcnmb start && rcsmb start` e fermarti con `rcsmb stop && rcnmb stop`.

Il file di configurazione centrale di Samba è `/etc/samba/smb.conf` che da un punto di vista logico si divide in due sezioni. Nella cosiddetta sezione `[global]` si effettuano le impostazioni principali e generali. La seconda sezione chiamata `[share]` contiene le singole share di file e stampanti. In tal modo, i det-

tagli riguardanti la share possono essere impostati singolarmente, oppure uniformemente nella sezione `[global]`. Ciò conferisce maggior chiarezza ai file di configurazione.

32.1.1 Sezione global

I seguenti parametri della sezione `[global]` devono essere adattati alle caratteristiche della vostra rete, affinché il vostro server Samba sia visibile tramite SMB per gli altri sistemi in un ambiente Windows.

workgroup = TUX-NET Con questa istruzione assegnate il server Samba ad un gruppo di lavoro. Sostituite a `TUX-NET` il gruppo di lavoro effettivo. Il server Samba in questa configurazione è visibile con il suo nome DNS nel gruppo di lavoro selezionato, sempre che il nome non sia stato già assegnato. Se il nome è già stato assegnato, con `netbiosname=MIONOME` potete impostare un nome che differisce dal nome DNS. Per maggiori dettagli a riguardo rimandiamo alla relativa pagina di manuale ovvero `man smb.conf`.

os level = 2 In base a questo parametro il server Samba decide se tentare di fungere da LMB (ingl. Local Master Browser) per il proprio gruppo di lavoro. Il valore utilizzato nell'esempio è stato scelto volutamente basso, per evitare che in una rete Windows si verifichino dei disturbi dovuti ad un server Samba configurato in modo errato. I dettagli su questo tema importante si trovano nei file `BROWSING.txt` e `BROWSING-Config.txt` nella sottodirectory `textdocs` della documentazione del pacchetto.

Se sulla vostra rete ancora non gira un server SMB (p.es. Windows NT o 2000 Server) ed il server Samba dovrà mettere a disposizione nella rete locale i nomi dei sistemi disponibili, aumentate il valore dell'`os level` (impostandolo ad es. su `65`), per fargli assumere il ruolo di LMB.

Siate cauti nel modificare questo valore, poiché potreste causare delle interferenze in una rete Windows. Consultatevi con il vostro amministratore di sistema, testate prima le modifiche in una rete isolata od in un momento poco critico.

wins support e server wins Volete integrare un server Samba in una rete Windows esistente, con un server WINS in esecuzione? Allora attivare il parametro `wins server` impostandolo sull'indirizzo IP del server WINS.

Se i vostri sistemi Windows sono in esecuzione in sottoreti distinte ma dovranno continuare ad essere indirizzabili tra di loro è necessario un server WINS. Per impostare il server Samba quale server WINS impostate `wins support = Yes`. Assicuratevi assolutamente che questo parametro sia attivato solo sul server Samba. Non abilitate mai contemporaneamente entrambe le opzioni `wins server` e `wins support` nel file di configurazione `smb.conf`.

32.1.2 Le share

Nei seguenti esempi dei client SMB condividono un lettore di CD-Rom e le directory `homes`.

`\mbox{[cdrom]}` Per evitare di sharare, ossia condividere, inavvertitamente un lettore di CD-ROM, tutte rispettive le righe sono disattivate (in questo caso con un punto e virgola). Se volete che il lettore di CD-Rom venga condiviso tramite Samba cancellate il punto e virgola (';') a inizio riga.

Esempio 32.1: *Condivisione del lettore di CD-Rom*

```
;[cdrom]
;       comment = Linux CD-ROM
;       path = /media/cdrom
;       locking = No
```

`[cdrom]` e `comment` La voce `[cdrom]` è il nome della share visibile ai client SMB. Con `comment` si può dare un nome espressivo alla risorsa condivisa.

`path = /media/cdrom` Con `path` viene esportata la directory `media/cdrom`.

Questo tipo di share è disponibile solo per gli utenti presenti sul sistema a causa della impostazione di default volutamente restrittiva. Se la share deve essere disponibile per tutti, bisogna aggiungere la riga `guest ok = Yes`. Visto che in tal modo tutti i membri della rete hanno il permesso di lettura, questa impostazione dovrebbe essere maneggiata con estrema cautela, ed essere applicata solo a determinate share; particolar attenzione va fatta se si intende utilizzare tale parametro nella sezione `[global]`.

[homes] Per la share `[homes]` vale: un utente si potrà collegare se dispone di un account e di una password valida per il server di file Linux nonché di una propria directory home.

Esempio 32.2: *Sharare gli home*

```
[homes]
        comment = Home Directories
        valid users = %S
        browseable = No
        read only = No
        create mask = 0640
        directory mask = 0750
```

[homes] Se non esiste una share con il nome share dell' utente che si connette al server SMB, viene generata dinamicamente una share in base alle direttive della share `[homes]`. Il nome della share sarà identico a quello dell'utente.

valid users = %S `%S` viene sostituito con il nome della share, una volta stabilito il collegamento. Visto che nel caso della share `[homes]` si tratta del nome dell'utente, il permesso di accesso l'ha solo il proprietario della directory utente.

browseable = No Con questa impostazione la share non è visibile sulla rete.

read only = No Di default, Samba non consente l' accesso in scrittura a share esportate, quindi si avrà `read only = Yes`. Se volete conferire l'accesso in scrittura ad una share, impostate `read only = No` che corrisponde a `writeable = Yes`.

create mask = 0640 I sistemi Windows non conoscono il concetto dei permessi d'accesso di Unix; quindi quando si crea un file non sono in grado di assegnare anche i permessi d'accesso. Il parametro `create mask` stabilisce con quali permessi di accesso debbano venire creati i file. Questo vale solo per share per le quali si ha accesso in scrittura. In questo caso, al proprietario viene dato il permesso di lettura e scrittura ed ai membri del gruppo primario del proprietario il permesso di lettura. Ricordate che `valid users = %S` non concede il permesso di lettura neanche se il gruppo ha il permesso di lettura. Di conseguenza si deve disabilitare la riga `valid users = %S` se si vuole concedere al gruppo l'accesso in lettura o scrittura.

32.1.3 Security Level

Il protocollo SMB proviene dal mondo di DOS/Windows e considera direttamente la questione della sicurezza. Ogni accesso ad una share può venire protetto da una password. SMB conosce tre possibilità per verificare il permesso di accesso:

Share level security (security = share):
Qui viene attribuita una password ad una share. Chi conosce la password, ha accesso alla share.

User level security (security = user): Questa variante introduce il concetto di utente. Ogni utente deve fare il login sul server immettendo una password. Dopo di ciò il server consente l'accesso alle singoli share esportate, in base al nome dell'utente.

Server level security (security = server):
Samba comunica al client di lavorare nel modo user level. In verità delega tutte le richieste di password ad un altro cosiddetto User Level Mode Server preposto all' autenticazione. Questa configurazione richiede un ulteriore parametro (`password server =`).

La distinzione fra share, user e server level security vale per l' intero server. Non è possibile esportare alcune share con share level security ed altre con user level security. Comunque su di un sistema potete avere un server Samba per ogni indirizzo IP configurato.

Per ulteriori informazioni rimandiamo alla Samba HOWTO Collection. Se amministrate diversi server su di un sistema dovete considerare i parametri `interfaces` e `bind interfaces only`.

Suggerimento

Per semplici interventi di natura amministrativa sul server Samba si propone il programma swat che mette a disposizione una interfaccia web intuitiva tramite la quale potrete configurare comodamente il server Samba. Invocate in un browser `http://localhost:901` ed eseguite il login come `root`. Tenete presente che swat è da abilitare anche nei file `/etc/xinetd.d/samba` e `/etc/services`, impostate a riguardo in `/etc/xinetd.d/samba` il seguente parametro: `disable` su `no`. Per maggiori informazioni su swat consultate la relativa pagina di manuale.

Suggerimento

32.2 Samba come server per il login

In reti composte principalmente da client Windows è spesso auspicabile che agli utenti sia concesso di eseguire il login solo se dispongono di account e password validi. Questo può venire realizzato con l'aiuto di un server Samba. In una rete puramente Windows questo compito viene svolto da un server Windows-NT configurato come cosiddetto Primary Domain Controller (PDC). Nella sezione `[global]` di `smb.conf` dovranno essere impostati i seguenti parametri, si veda l'esempio 32.3 in questa pagina:

Esempio 32.3: *Sezione globale in smb.conf*

```
[global]
        workgroup = TUX-NET
        domain logons = Yes
        domain master = Yes
```

Se ai fine della verifica vengono usate password cifrate - questo è lo standard con versioni aggiornate di MS Windows 9x, MS Windows NT 4.0 a partire dal service pack 3 e versioni di prodotto successive - il server Samba deve essere in grado di amministrarle, cosa che avviene tramite la registrazione `encrypt passwords = yes` nella sezione `[global]`, impostazione che si ha di default a partire dalla versione 3 di Samba; inoltre gli account e le password degli utenti devono venire convertiti in una forma cifrata conforme a Windows. Questo avviene con il comando `smbpasswd-a name`. Poiché secondo il concetto di dominio di Windows NT, anche i computer necessitano di un account di dominio, createlo con i seguenti comandi:

Esempio 32.4: *Creare un account macchina*

```
useradd nomehost\$
smbpasswd -a -m nomehost
```

Ad `useradd` è stato aggiunto un simbolo del dollaro. Il comando `smbpasswd` lo aggiunge da sé quando si usa il parametro `-m`. Nella configurazione esempio commentata `/usr/share/doc/packages/samba/examples/smb.conf.SuSE` vi sono delle impostazioni che automatizzano questi processi.

Esempio 32.5: *Creare automaticamente un account macchina*

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" \
-s /bin/false %m\$
```

Affinché Samba esegua in modo corretto questo script è richiesto un utente Samba con i diritti di amministratore. Selezionate un utente ed aggiungetelo al gruppo `ntadmin`. In seguito potrete assegnare a tutti gli utenti di questo gruppo Unix lo stato `Domain Admin` tramite:

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

Per maggiori informazioni rimandiamo capitolo 12 della Samba HOWTO Collection che trovate sotto: `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

32.3 Installazione e configurazione con YaST

Iniziate la configurazione del server con la selezione del gruppo di lavoro o dominio gestito dal vostro server Samba. Potete selezionare un gruppo di lavoro/dominio dal menu a tendina 'Nome del gruppo di lavoro o dominio' o immetterne uno nuovo. Successivamente specificate se il vostro server debba fungere da PDC (primary domain controller) o da BDC (backup domain controller).

Nel menu 'Avvio' (si veda la figura 32.1 nella pagina successiva) selezionate se avviare Samba, in caso affermativo il servizio viene inizializzato ad ogni avvio del sistema. Tramite 'Porte aperte nel firewall' e 'Dettagli firewall' adattate il firewall in esecuzione sul server in modo che le porte per i servizi `netbios-ns`, `netbios-dgm`, `netbios-ssn` e `microsoft-ds` siano aperte su tutte le interfacce interne e esterne in modo da assicurare un funzionamento senza intoppi del server Samba.

Nel menu 'Shares' (si veda la figura 32.2 a pagina 577) determinate quali share Samba abilitare. Tramite 'Cambia stato' potete passare da uno stato all'altro, ovvero da 'Abilitato' a 'Disabilitato' e viceversa. Nuove share vanno aggiunte tramite 'Aggiungi'.

Nel menu 'Identità' (si veda la figura 32.3 a pagina 578) stabilite il dominio di appartenenza dell'host ('Impostazioni di base') e se va utilizzato un nome host alternativo nella rete ('Nome NetBIOS').

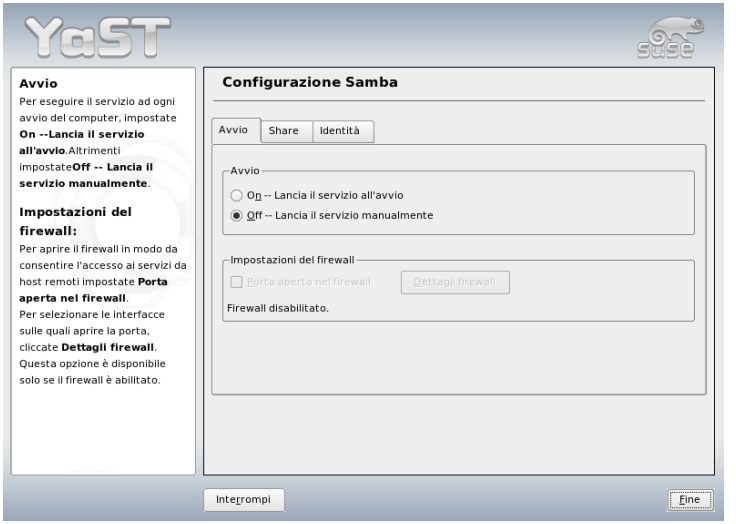

Figura 32.1: *Configurazione Samba*

32.4 Configurazione dei client

I client possono indirizzare il server Samba solo tramite TCP/IP. NetBEUI o NetBIOS via IPX non sono utilizzabili con Samba.

32.4.1 Configurazione di un client Samba tramite YaST

Configurate un client Samba per potere accedere in modo semplice a risorse (file o stampante) sul server Samba. Nella finestra 'Gruppo di lavoro Samba' indicate il dominio e il gruppo di lavoro. Tramite 'Seleziona' vengono indicati tutti i gruppi e domini disponibili. Potete fare le vostre selezioni con un clic di mouse. Abilitate la casella 'Utilizzare informazioni SMB per l'autenticazione Linux' e l'autenticazione degli utenti verrà eseguita tramite il server Samba. Dopo aver completato le impostazioni, fate clic su 'Fine' per concludere il processo di configurazione.

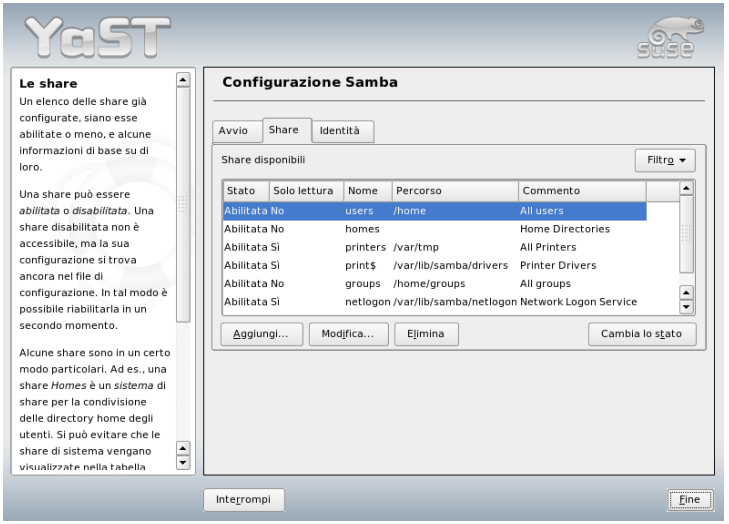

Figura 32.2: *Configurazione Samba: le share*

32.4.2 Windows 9x/ME

Windows 9x/ME supporta TCP/IP. Comunque tale supporto non viene installato di default. Per abilitare successivamente il supporto a TCP/IP, si va su 'Pannello di controllo' → 'Sistema' e quindi si seleziona 'Aggiungi' → 'Protocolli' → 'TCP/IP di Microsoft'. Dopo un reboot del computer Windows, eseguite un doppio clic sul simbolo del desktop per l'ambiente di rete per visualizzare il server Samba.

Suggerimento

Per utilizzare una stampante sul server Samba si dovrebbe installare il driver di stampante PostScript standard o quello della Apple per la relativa versione di Windows; si consiglia di scegliere una coda di stampa Linux che accetta PostScript quale formato di input.

Suggerimento

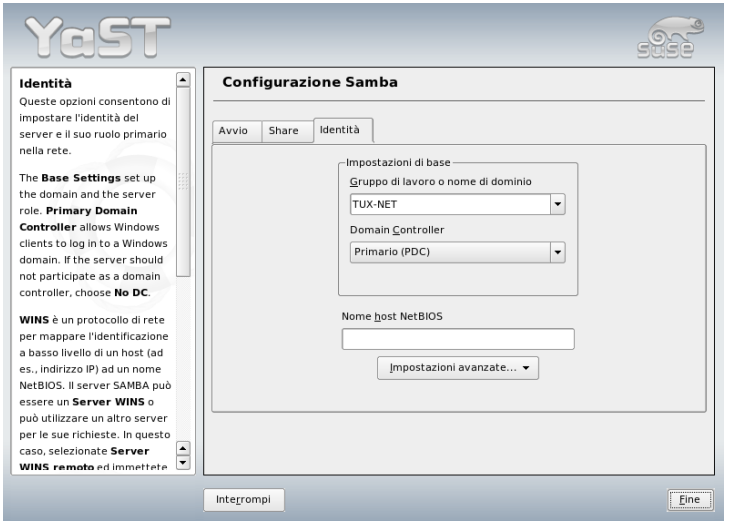

Figura 32.3: *Configurazione Samba: identità*

32.5 Ottimizzazione

`socket options` offre modo di eseguire delle ottimizzazioni. Le impostazioni di default nella configurazione esempio fornita a corredo si basano su una rete Ethernet locale. Ulteriori dettagli su `socket options` sono reperibili nella pagina di manuale di `smb.conf`, nella sezione dedicata a questa tematica e nella pagina di manuale `socket(7)`. Per ulteriori informazioni consultate anche il capitolo `Samba performance tuning` della Samba HOWTO Collection.

La configurazione di default in `/etc/samba/smb.conf` cerca di proporre dei valori sensati e si orienta alle preimpostazioni del Samba team. Comunque non è possibile avere subito una configurazione pronta per l'uso, in particolar modo per ciò che riguarda la configurazione di rete ed il nome del gruppo di lavoro. Nella configurazione esempio commentata in `examples/smb.conf.SuSE` trovate tante indicazioni utili per gli adattamenti del caso.

Suggerimento

Il Samba team fornisce nella Samba HOWTO Collection una sezione dedicata al rilevamento di errori. Part V contiene inoltre delle istruzioni da seguire passo per passo per controllare la configurazione.

Suggerimento

Server proxy: Squid

Squid è una cache-proxy molto diffusa per piattaforme Linux/UNIX. Descriveremo come configurarla, i requisiti di sistema necessari, come configurare il proprio sistema per poter eseguire un proxying trasparente ed infine come fare per ottenere statistiche sul carico della cache con l'aiuto di programmi come Calamaris e cachemgr o come filtrare contenuti web con squidGuard.

33.1 Cos'è una cache-proxy?

Squid funge da cache di proxy. Inoltra le richieste di oggetti da parte dei client (in questo caso browser web) al server competente. Quando arrivano gli oggetti richiesti dal server, passa gli oggetti ai client e ritiene una copia degli oggetti nella cache del disco rigido. Il vantaggio è che quando più client richiedono lo stesso oggetto sarà la cache del disco rigido a replicare, quindi il processo è molto più veloce che nel caso di una richiesta inviata su Internet ed inoltre si riduce notevolmente il traffico di rete.

Squid offre un vasto spettro di proprietà, oltre al caching; p.es. permette di definire gerarchie di server proxy per il bilanciamento del carico di sistema, designare regole di accesso fisse per tutti i client che vogliono accedere al proxy, consentire o negare l'accesso a determinate pagine web con l'aiuto di altre applicazioni o fornire delle statistiche sulle pagine web maggiormente visitate e quindi di valutare il comportamento di navigazione degli utenti su Internet. Squid non è un proxy generico; normalmente fa solo da mediatore fra i collegamenti HTTP. Inoltre appoggia i protocolli FTP, Gopher, SSL e WAIS, ma non altri protocolli Internet come Real Audio, News o videoconferenze. Squid usa il protocollo UDP solo per supportare la comunicazione fra diverse cache, questo è il motivo per cui non vengono supportati diversi programmi multi-media.

33.2 Informazioni sulla cache proxy

33.2.1 Squid e la sicurezza

Squid può essere usato insieme ad un firewall per proteggere reti interne da attacchi dall'esterno attraverso l'uso di un proxy cache. Il firewall, fatta eccezione per Squid, nega ai client di collegarsi a dei servizi esterni; tutte le connessioni al World Wide Web devono essere stabilite attraverso il proxy.

Nel caso di una configurazione firewall con una DMZ (zona demilitarizzata), imposteremo lì il nostro proxy: in un assetto configurativo del genere è essenziale che tutti i computer nella DMZ mandino i loro file di protocollo ai computer che si trovano all'interno della rete protetta. Come impostare il cosidetto proxing "trasparente" viene illustrato nella sezione 33.6 a pagina 592.

33.2.2 Diverse cache

I proxy si lasciano configurare in modo che scambiano degli oggetti tra di loro per ridurre così il carico del sistema ed aumentare la possibilità di trovare un oggetto già esistente nella rete locale. Questo concetto permette anche la configurazione di gerarchie di cache, cosicché una cache è in grado di inoltrare richieste di oggetti a cache della stessa gerarchia, o indurre una cache superiore (nella gerarchia) a recuperare gli oggetti da un'altra cache nella rete locale o direttamente dalla fonte.

La scelta della topologia giusta per la gerarchia della cache è molto importante allo scopo di impedire un aumento complessivo del traffico di rete. In una grande rete, è p.es. possibile configurare un server proxy per ogni sottorete e collegarlo poi con il proxy superiore, il quale a sua volta è collegato alla cache del proxy dell'ISP.

L'intera comunicazione viene controllata da ICP (ingl. Internet Cache Protocol), che è basato sul protocollo UDP. Lo scambio di dati fra le cache avviene tramite HTTP (ingl. Hyper Text Transmission Protocol) che si basa su TCP.

Per trovare il server più appropriato per gli oggetti desiderati, la cache invia una richiesta ICP a tutti i proxy della stessa gerarchia. Se l'oggetto è stato trovato, i proxy replicano tramite risposte ICP alle richieste con il codice "HIT"; se non è stato trovato nulla, rispondono con il codice "MISS". Nel caso di più risposte HIT, il server proxy incaricherà un server ad eseguire il download: questa decisione viene determinata fra l'altro dalla cache che invia come prima la risposta o dalla prossimità della cache. Se non viene inviata alcuna risposta soddisfacente, la richiesta viene inviata alla cache superiore.

Suggerimento

Per evitare la molteplice memorizzazione di oggetti in diverse cache della nostra rete, vengono usati altri protocolli ICP come p.es. CARP (ingl. Cache Array Routing Protocol o HTCP (ingl. Hyper-Text Cache Protocol). Più oggetti si trovano nella nostra rete, più grande sarà la possibilità di trovare quello cercato.

Suggerimento

33.2.3 Buffering di oggetti scaricati da Internet

Non tutti gli oggetti disponibili nella rete sono statici; vi sono molte pagine CGI generate dinamicamente, i contatori di accesso o i documenti SSL cifrati per una

maggiore sicurezza. Per questo motivo, tali oggetti non vengono conservati nella cache, dato che l'oggetto ad ogni nuovo accesso si è già modificato.

Per tutti gli altri oggetti nella cache si pone comunque la domanda: per quanto tempo debbano rimanervi? Per facilitare questa decisione, gli oggetti vengono assegnati a tre stadi diversi: Attraverso header o intestazioni come `Last modified` ("modificato recentemente") o `Expires` ("scade") e la data corrispondente, i server web e proxy si informano sullo stato di un oggetto. Vengono usati anche altri header che p.es. indicano oggetti da non memorizzare temporaneamente.

Gli oggetti nella cache di solito vengono sostituiti a causa della mancanza di spazio di memoria attraverso algoritmi del tipo LRU (ingl. Last Recently Used) che sono stati concepiti per sostituire oggetti della cache. Il principio è quello di sostituire come primo gli oggetti meno richiesti.

33.3 Requisiti di sistema

Innanzitutto dovrebbe venire stabilito il carico massimo del sistema: a questo scopo, è importante dare più peso alle punte di carico del sistema, poiché queste possono essere di quattro volte maggiori della media giornaliera. In caso di dubbio, è consigliabile non essere avari in questi casi, dato che uno Squid al limite delle sue prestazioni potrebbe comportare un notevole abbassamento della qualità del servizio. Vi elencheremo ora i diversi requisiti di sistema in ordine di importanza.

33.3.1 Disco rigido

Per memorizzare temporaneamente, la velocità investe un ruolo molto importante; badate quindi in particolare modo a questo fattore. Nei dischi rigidi, questo parametro è indicato come *tempo di posizionamento* espresso in millesimi di secondo. Una regola approssimativa: più basso è questo valore e meglio è. Dato che Squid il più delle volte legge dal o scrive sul disco rigido piccoli blocchi di dati, la velocità di posizionamento è più rilevante della velocità della trasmissione dei dati (throughput). Proprio in casi come questi vale la pena avere dei dischi rigidi con un numero di giri elevato che consentono di posizionare velocemente la testina del disco. Dischi SCSI veloci hanno ad esempio un tempo di accesso al di sotto di 4 millesimi di secondo. Un altro espediente per aumentare la velocità di trasmissione dei dati consiste nell'usare contemporaneamente più dischi rigidi o Raid Array stripes.

33.3.2 Dimensioni della cache del disco rigido

La probabilità di un HIT (l'oggetto desiderato si trova già nella cache) in una cache piccola è molto scarsa, perché si riempirà molto velocemente. In questo caso, gli oggetti poco richiesti, vengono sostituiti da nuovi. Se la cache ha però a disposizione 1 Gbyte e gli utenti necessitano di 10 Mbyte al giorno per navigare su Internet, per riempire la cache occorreranno più di 100 giorni.

La dimensione della cache può venire facilmente determinata tramite la velocità di trasmissione massima del collegamento. Con un collegamento di 1Mbit/s il tasso di trasmissione massimo è di 125 Kbyte/s. Se il traffico completo dei dati arriva nella cache, entro un'ora avremo un totale di 450 Mbyte. Partendo dal presupposto che il completo traffico dei dati si svolga entro 8 ore di lavoro, in un giorno avremo "raccimolato" 3,6 Gbyte. Poiché di solito il collegamento non viene sfruttato fino in fondo, possiamo partire dal presupposto che la quantità di dati che passa attraverso la nostra cache, sia di ca. 2 Gbyte. Nel nostro esempio, abbiamo bisogno di 2 Gbyte di memoria per Squid per mantenere nella cache i dati di tutte le pagine visitate durante *un* giorno.

33.3.3 RAM

La memoria (RAM) necessaria a Squid dipende dal numero degli oggetti che si trovano nella cache. Affinché i dati possano venire richiesti più velocemente, Squid salva anche nella memoria i cache object pointer ed i dati richiesti più spesso. La RAM è molto più veloce del disco rigido!

Squid tiene in memoria anche molti altri dati, come p.es. una tabella con tutti gli indirizzi IP assegnati, una ben determinata cache per nomi di domini, gli oggetti più richiesti, buffer, ACL, etc.

E' molto importante avere sufficiente memoria per un processo Squid: se dovesse venire trasferito sul disco rigido, il rendimento del sistema verrebbe drasticamente ridotto. Per l'amministrazione della memoria della cache, vi è il tool cachemgr.cgi che tratteremo nella sezione 33.7 a pagina 595.

33.3.4 CPU

Il programma Squid non ha bisogno di molta CPU. I picchi di carico per il processore si hanno solo all'avvio e durante il controllo del contenuto della cache. L'impiego di un computer multi-processore non aumenta la prestazione del sistema. Per aumentare l'effettività si devono usare dischi rigidi più veloci o aggiungere memoria.

33.4 Avviare Squid

Lo Squid su SUSE LINUX è già preconfigurato e può essere utilizzato ad installazione avvenuta. Premessa per un avvio senza complicazioni: la rete deve essere configurata in modo che siano raggiungibili almeno un server dei nomi ed Internet. Potrebbe essere problematico, se si utilizza un collegamento con una configurazione DNS dinamica: in questo caso, almeno il server dei nomi dovrebbe essere registrato in maniera permanente, poichè Squid non parte se non trova alcun server DNS in `/etc/resolv.conf`.

33.4.1 Fermare e avviare Squid

Per avviare Squid inserite (come `root`) nella riga di comando: `rcsquid start`. Al primissimo avvio, viene prima creata la struttura di directory in `/var/squid/cache`; ciò viene realizzato automaticamente dallo script di avvio `/etc/init.d/squid` e può durare un paio di secondi. Se sulla destra, viene visualizzato un `done` color verde, vuol dire che Squid è stato avviato correttamente. Sul sistema locale è possibile collaudare subito il funzionamento di Squid, immettendo nel browser come proxy `localhost` e `3128` quale porta.

Per permettere a tutti l'accesso a Squid, e quindi anche ad Internet, basta modificare nel file di configurazione `/etc/squid.conf` la registrazione da `http_access deny all` a `http_access allow all`. Tenete però presente che, in questo modo, aprite Squid a tutti; è quindi necessario definire delle ACL che regolano l'accesso al proxy. Per maggiori approfondimenti, si veda la sezione 33.5.2 a pagina 589.

Se si sono eseguite delle modifiche nel file di configurazione `/etc/squid.conf`, Squid dovrà ricaricare il file di configurazione. Questo avviene con il comando: `rcsquid reload`. Alternativamente, potete riavviare Squid con: `rcsquid restart`.

Importante è anche questo comando: `rcsquid status`. Con esso si può stabilire se il proxy è in esecuzione, e con `rcsquid stop` si può fermare Squid. Questo può durare un po', poiché Squid aspetta fino ad un mezzo minuto (opzione `shutdown_lifetime` in `/etc/squid.conf`), prima di interrompere i collegamenti con i client e di scrivere i suoi dati sul disco rigido.

Avvertimento

Terminare Squid

Se chiudete Squid con un `kill` o `killall`, ciò può danneggiare la cache. Per riavviare Squid bisogna cancellarla completamente.

Avvertimento

Se dopo un pò Squid si chiude, nonostante l' avvio sia apparentemente riuscito, questo può essere dovuto ad una registrazione del server dei nomi errata o alla mancanza di un `/etc/resolv.conf`. Squid protocolla nel file `/var/squid/logs/cache.log` la causa di un avvio fallito. Se Squid deve venire avviato automaticamente al boot, nell'editor dei runlevel di bisogna attivare Squid per i runlevel in questione. Si veda la sezione 2.7.7 a pagina 78

Se disinstallate Squid, la cache e i file di log rimangono; dunque, si dovrà cancellare manualmente la directory `/var/cache/squid`.

33.4.2 Server DNS locale

E' consigliabile impostare un server DNS locale anche se non dovete gestire un proprio dominio. Fungerà da server dei nomi cosiddetto caching-only e consentirà di risolvere delle richieste DNS tramite server dei nomi root senza richiedere una particolare configurazione (si veda la sezione 24.2 a pagina 451). Il modo di realizzare ciò dipende se selezionate o meno il DNS dinamico durante la configurazione della connessione ad Internet.

DNS dinamico Di solito con il DNS dinamico il server DNS viene impostato dal provider durante la connessione ad Internet ed il file locale `/etc/resolv.conf` viene adattato in modo automatico. Ciò viene realizzato tramite la variabile di sysconfig `MODIFY_RESOLV_CONF_DYNAMICALLY` che viene impostata su `YES`. Potete impostare questa variabile su `NO` servendovi dell'editori sysconfig di YaST (si veda la sezione 7.8 a pagina 174). Immettete quindi il server DNS locale nel file `/etc/resolv.conf` utilizzando l'indirizzo IP `127.0.0.1` per `localhost`. In questo modo Squid è in grado di rilevare il server dei nomi locali al suo avvio.

Per accedere al server di nomi del provider, inseritene il nome nel file di configurazione `/etc/named.conf` sotto `forwarders` specificando inoltre l'indirizzo IP. Il DNS dinamico consente di realizzare ciò in modo automatico durante la connessione tramite la variabile sysconfig `MODIFY_NAMED_CONF_DYNAMICALLY` che va impostata su `YES`.

DNS statico Con DNS statico non vi sono degli adattamenti automatici riguardo a DNS in fase di collegamento; quindi non server modificare le variabili sysconfig, ma dovete immettere il server DNS locale nel file `/etc/resolv.conf` come descritto sopra. Ulteriori server dei nomi statici vanno immessi manualmente nel file `/etc/named.conf` sotto `forwarders` con rispettivo indirizzo IP.

Suggerimento

DNS e firewall

Se avete attivato un firewall, assicurate che le richieste DNS non vengano bloccate dal firewall.

Suggerimento

33.5 Il file di configurazione /etc/squid/squid.conf

Tutte le impostazioni del server proxy Squid devono venire eseguite nel file `/etc/squid/squid.conf`; per poter inizializzare Squid per la primissima volta, non è necessario eseguirvi alcuna modifica, ma, in un primo momento, è vietato l'accesso ai client esterni. Il proxy è abilitato per `localhost` e, come porta, viene usata di norma `3128`. Le opzioni sono documentate dettagliatamente con numerosi esempi nel file preinstallato `/etc/squid/squid.conf`. Quasi tutte le righe hanno all'inizio il segno di commento #, mentre, alla fine della riga, troverete le relative specificazioni. I valori indicati corrispondono quasi sempre ai valori preimpostati, cosicché l' eliminazione del carattere di commento, senza la modifica del parametro dell'opzione, non ha alcun effetto – fatte poche eccezioni. Si consiglia lasciare invariato l'esempio ed inserire l'opzione con il parametro modificato in una riga inferiore. In questo modo, si vedono i valori preimpostati e le modifiche.

Suggerimento

Adattare il file di configurazione a seguito di un update

Se si esegue un aggiornamento di Squid si consiglia assolutamente di utilizzare il nuovo `/etc/squid/squid.conf` e di assumere solo le modifiche del file originario. Se tentate di continuare a utilizzare il vecchio file `squid.conf` correte pericolo che la configurazione non funzioni più, visto che le opzioni si modificano e se ne aggiungono delle nuove continuamente.

Suggerimento

33.5.1 Opzioni generali di configurazione (selezione)

http_port 3128 La porta sulla quale Squid si mette "in ascolto" per richieste dei client. E' preimpostata su `3128`, ma viene usata anche `8080`. Qui è possibile indicare più numeri di porte, divisi da uno spazio.

cache_peer ⟨***nome_host***⟩ ⟨***type***⟩ ⟨***proxy-port***⟩ ⟨***icp-port***⟩
Qui è possibile indicare un proxy superiore come "parent" (genitore), p.es. se si vuole o si deve usare il proxy del provider. Come ⟨*nome host*⟩ si registra il nome o l'indirizzo IP del proxy da usare e come ⟨*type*⟩ `parent`. Per ⟨*proxy-port*⟩ si digita il numero della porta che l'utente del parent indica anche per l'uso nel browser; nella maggior parte dei casi `8080`. ⟨*icp-port*⟩ si può impostare su `7` o su `0` se non è nota la porta ICP del parent e non ne è stato concordato l'uso con il provider. Inoltre, dopo il numero della porta si deve anche indicare `default` e `no-query`, per impedire completamente l'uso del protocollo ICP. Dopo di ciò, nei confronti del proxy del provider, Squid si comporterà come un normale browser.

cache_mem 8 Mbyte Questa registrazione indica il massimo di RAM usata da Squid per il caching. La preimpostazione è di `8 Mbyte`.

cache_dir ufs /var/cache/squid 100 16 256
La registrazione *cache_dir* indica la directory dove gli oggetti vengono archiviati sul disco rigido. I numeri posposti indicano lo spazio massimo utilizzabile in "Mbyte" e il numero quantità di directory nel primo e secondo livello. Il parametro `ufs` dovrebbe rimanere invariato. Nella directory `/var/squid/cache` sono preimpostati "100 Mbyte" di memoria del disco rigido da occupare e vi possono venire create 16 sottodirectory

che a loro volta contengono 256 directory. All'indicazione della memoria da utilizzare, si devono lasciare riserve sufficienti; ragionevoli i valori fra il 50% e massimo l'80% dello spazio disponibile. É bene essere molto prudenti con l'aumento della quantità delle directory, poiché troppe directory possono causare problemi di prestazioni. Se esistono più dischi rigidi sui quali distribuire la cache, è possibile registrare diverse righe *cache_dir* .

cache_access_log /var/squid/logs/access.log
Percorso per i file di log.

cache_log /var/squid/logs/cache.log Percorso per i file di log.

cache_store_log /var/squid/logs/store.log
Percorso per i messaggi di log.

Queste registrazioni indicano il percorso al file di protocollo di Squid. Di solito si lasciano invariate. Se Squid è molto carico, può essere consigliabile distribuire la cache e i file di log su diversi dischi rigidi.

emulate_httpd_log off Se si cambia la registrazione in *on*, si ottengono file di log leggibili. Alcuni programmi non riescono ad elaborarli correttamente.

client_netmask 255.255.255.255 Con questa registrazione è possibile mascherare nei file di log gli indirizzi IP per celare l'identità del client. Se qui viene registrato `255.255.255.0`, l'ultima cifra dell'indirizzo IP viene impostata su zero.

ftp_user Squid@ Specificare qui la password che Squid debba usare per i login FTP anonimi. Alternativamente, potete indicare anche un indirizzo e-mail valido del vostro dominio, dal momento che alcuni server FTP ne verificano la validità.

cache_mgr webmaster Si tratta di un indirizzo e-mail al quale Squid invia una messaggio nel caso di un crollo inaspettato. Di default si ha *webmaster*.

logfile_rotate 0 Se si invoca `squid -k rotate`, `Squid` è in grado di ruotare i file di log memorizzati: i file vengono numerati e, dopo aver raggiunto il valore indicato, il file più vecchio viene sovrascritto. Di norma, questo valore è impostato su `0`, perché l'archiviazione e l'eliminazione dei file log vengono eseguite da un job di cron configurato nel file `/etc/logrotate/squid`.

append_domain <dominio> Con *append_domain* si può indicare quale dominio venga automaticamente aggiunto, se non se ne è indicato alcuno. Nella maggior parte dei casi, qui viene indicato il proprio dominio, dopo di ciò, per raggiungere il proprio server web è sufficiente indicare *www* nel browser.

forwarded_for on Se si imposta questa registrazione su *off*, Squid rimuove dalle richieste HTTP, l'indirizzo IP o il nome del sistema del client.

negative_ttl 5 minutes; negative_dns_ttl 5 minutes
Normalmente non è necessario modificare questi valori. Nel caso di una connessione dial-up, può accadere che Internet risulti per un pò non accessibile: Squid si ricorda delle richieste andate a vuoto e si rifiuta di ripeterle, benché il collegamento con Internet sia nuovamente attivo. In questi casi, si possono impostare i *minutes* su *seconds* cosicchè, pochi secondi dopo la connessione, anche un *Reload* nel browser porta all'effetto desiderato.

never_direct allow ⟨***acl_name***⟩ Se si vuole evitare che Squid invii direttamente le sue richieste ad Internet, con la registrazione sopra citata, si può forzare l'impiego di un altro proxy, che deve prima essere stato registrato sotto *cache_peer* . Se si seleziona ⟨*acl_name*⟩ `all`, tutte le richieste vengono inoltrate direttamente al *parent*. Ciò può essere necessario se p.es. si utilizza un provider che prescrive l'uso del suo proxy o se il firewall non consente alcun accesso diretto ad Internet.

33.5.2 Opzioni per le ACL

Squid offre un raffinato sistema per controllare l'accesso al proxy, che con le ACL si lascia configurare in modo versatile. Si tratta di elenchi di regole che vengono elaborate l'una dopo l'altra. Prima di usarle, le ACL vanno definite. Alcune ACL standard come *all* e *localhost* esistono già. Di per sé, la definizione di una ACL non ha ancora nessuna conseguenza: solo quando viene usata assieme alle regole definite in *http_access* vengono applicate effettivamente.

acl <acl_name> <type> <data> Per essere definita una ACL ha bisogno di almeno tre dati: il nome <*acl_name*> che può venire scelto liberamente. Per <*type*> è possibile scegliere fra un numero di possibilità diverse che trovate nella sezione *ACCESS CONTROLS* in `/etc/squid/squid.conf`. Cosa indicare per <*data*> dipende dal tipo di ACL e può essere letto anche da un file, p.es. tramite nome di computer, indirizzo IP o URL. Eccovi qui di seguito alcuni semplici esempi:

```
acl i-miei-navigatori srcdomain .mio-dominio.com
acl insegnante src 192.168.1.0/255.255.255.0
acl studenti src 192.168.7.0-192.168.9.0/255.255.255.0
acl mezzogiorno time MTWHF 12:00-15:00
```

http_access allow <acl_name> Con *http_access* viene stabilito chi possa usare il proxy e a cosa ha il permesso di accedere su Internet: devono venire indicate le ACL, *localhost* e *all* sono già stati definiti sopra, che con *deny* o *allow* bloccano o consentono l'accesso. Qui è possibile creare una lista con parecchie registrazioni *http_access* che vengono elaborate dalla prima all'ultima; a seconda della registrazione, viene dato il via libera o bloccato l'accesso all'URL richiesta. La registrazione *http_access deny all* dovrebbe sempre essere all'ultimo posto. Nel seguente esempio, *localhost*, il computer locale, può accedere liberamente a tutto, mentre gli altri non possono accedervi.

```
http_access allow  localhost
http_access deny all
```

Ancora un esempio, nel quale vengono usate le ACL definite prima: il gruppo `insegnanti` ha sempre accesso ad Internet, mentre il gruppo `studenti` vi può navigare solo da lunedì a venerdì e solo a mezzogiorno.

```
http_access deny localhost
http_access allow insegnante
http_access allow studenti mezzogiorno
http_access deny all
```

Per motivi di maggior chiarezza, la lista con registrazioni *http_access* proprie dovrebbe venire inserita solo nello spazio previsto in `/etc/squid.conf`. Cioé fra il testo

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
# CLIENTS
```

ed il conclusivo

```
http_access deny all
```

redirect_program /usr/bin/squidGuard
Con questa opzione, è possibile indicare un "redirector", come, p.es., SquidGuard, che sia in grado di bloccare URL indesiderate. Assieme all' autenticazione proxy e le relative ACL, è possibile regolare in modo molto mirato l'accesso ad Internet da parte dei diversi gruppi di utenti.

SquidGuard è un pacchetto a sé stante che va installato e configurato a parte.

auth_param basic program /usr/sbin/pam_auth
Se si vuole che gli utenti si autenticano sul proxy, si può indicare qui un programma adeguato, p.es. pam_auth. Con pam_auth, al suo primo accesso, l'utente ha una finestra di login nella quale deve inserire l'user ID e la password: oltre a ciò è necessario anche una ACL affinché possano navigare solo i client con login valido:

```
acl password proxy_auth REQUIRED

http_access allow password
http_access deny all
```

Quel *REQUIRED* dopo *proxy_auth* può anche essere sostituito con una lista di nomi di utenti autorizzati o il percorso che conduce ad una lista del genere.

ident_lookup_access allow <acl_name>
In questo modo, è possibile far eseguire una richiesta ident per tutti gli utenti definiti tramite l'ACL, allo scopo di accertare l'identità del rispettivo utente. Se per *<acl_name>* si inserisce *all* , questo accertamento viene eseguito per tutti i client. A questo scopo, sui client deve girare un cosiddetto 'ident daemon'; per Linux, si può installare a questo proposito il pacchetto pidentd, per `Windows` esiste del software libero che può venire scaricato da Internet. Affinchè vengano ammessi solo i client la cui identità è stata accertata, deve venire definita una apposita ACL:

```
acl identhosts ident REQUIRED

http_access allow identhosts
http_access deny all
```

Anche qui *REQUIRED* può venire sostituito da un elenco di user ID consentiti. L'uso di *Ident* può rallentare notevolmente l'accesso, poiché l' identità viene accertata ad ogni richiesta.

33.6 Configurazione del proxying trasparente

Normalmente il browser web invia richieste ad una determinata porta del server proxy ed il proxy mette a disposizione gli oggetti richiesti, sia che si trovino nella cache o meno. All'interno di una rete vera possono verificarsi diverse situazioni:

- Per ragioni di sicurezza è bene che tutti i client usino un proxy per navigare su Internet.
- E' necessario che tutti i client utilizzino - consapevolmente o meno - un proxy.
- Il proxy è stato trasferito da un'altra parte all'interno della rete, ma i client esistenti devono mantenere la loro vecchia configurazione.

In ognuno di questi casi, può venire impiegato un proxy trasparente. Il principio è molto semplice: il proxy riceve le richieste del browser web e le elabora, cosicchè il browser web riceve le pagine richieste senza sapere da dove provengono. Tutto il processo viene eseguito in modo trasparente; da qui il nome del procedimento.

33.6.1 Configurazione del kernel

Prima assicuratevi che il kernel del server proxy supporti il proxing trasparente. Il kernel di SUSE LINUX è stato configurato in tal senso. Altrimenti dovete aggiungere questa opzione al kernel e ricompilarlo. Informazioni più precise a riguardo nel capitolo 9 a pagina 199.

33.6.2 Opzioni di configurazione in /etc/squid.conf

Nel file `/etc/squid/squid.conf` devono essere abilitate le seguenti opzioni per avere un proxy trasparente:

- `httpd_accel_host` virtual
- `httpd_accel_port` 80

  Porta sulla quale si trova il vero server HTTP.

- `httpd_accel_with_proxy` on
- `httpd_accel_uses_host_header` on

33.6.3 Configurazione del firewall con SuSEfirewall2

Tutte le richieste in arrivo che attraversano il firewall devono essere inoltrate, in base ad una regola di inoltro valida per le porte, alla porta Squid. A questo scopo, viene usato un tool fornito a corredo: SuSEfirewall2, il cui file di configurazione si trova in `/etc/sysconfig/SuSEfirewall2`. Il file di configurazione è composto da registrazioni ben documentate. Anche se intendete configurare solo un proxy trasparente, dovete configurare alcune opzioni inerenti al firewall, p.es.:

- Dispositivo che punta su Internet: `FW_DEV_EXT`="eth1"
- Dispositivo che punta sulla rete: `FW_DEV_INT`="eth0"

Alle porte ed ai servizi (si veda `/etc/services`) dietro il firewall accedono delle reti inaffidabili come Internet. Nel seguente esempio, offriamo solo servizi web verso l'esterno:

```
FW_SERVICES_EXT_TCP="www"
```

Definite le porte ed i servizi (si veda `/etc/services`) sul firewall alle quali si accede da reti (interne) sicure, sia tramite TCP che UDP.

```
FW_SERVICES_INT_TCP="domain www 3128"
FW_SERVICES_INT_UDP="domain"
```

Accediamo ai servizi web e a Squid (la cui porta standard è `3128`). Il servizio sopra descritto "Domain" sta per DNS o Domain Name Server: è usuale utilizzarlo. Diversamente toglietelo dalla registrazione di cui sopra e impostate l'opzione su `no`:

```
FW_SERVICE_DNS="yes"
```

L'opzione più importante è la cifra `15`:

Esempio 33.1: *Opzione 15 della configurazione del firewall*

```
#
# 15.)
# Quale accesso ai singoli servizi deve venire reindirizzato ad una
# porta locale sul computer firewall?
#
# Con ciò, tutti gli utenti esterni possono venire costretti a
# navigare tramite lo Squid Proxy oppure è possibile reindirizzare in
# maniera trasparente il traffico web entrante ad un server web
# sicuro.
#
# Scelta: non  eseguire alcuna registrazione o usare la sintassi
# delle regole di reindirizzo spiegata qui di seguito e divisa da
# uno spazio vuoto. Una regola di reindirizzo consiste in 1)
# IP/rete di origine, 2) IP/rete meta, 3) porta meta originaria e
# 4) porta locale alla quale deve venire reindirizzato il traffico,
# separato da virgole, p.es. "10.0.0.0/8,0/0,80,3128
# 0/0,172.20.1.1,80,8080"
#
```

Nel commento sopra riportato, viene mostrata la sintassi da rispettare. Immettete innazitutto l'indirizzo IP e la maschera di rete della "rete interna" che accede al firewall del proxy: quindi l'indirizzo IP e la maschere di rete ai quali i client inviano le richieste. Nel caso dei browser, stabiliamo le reti `0/0`; si tratta di una wildcard e significa "dappertutto". Segue la porta "originale", alla quale sono state spedite queste richieste, e, infine, segue la porta a cui sono state reindirizzate le richieste. Dal momento che Squid non supporta solo il protocollo HTTP, potete reindirizzare al proxy anche le richieste da altre porte, come FTP (porta 21), HTTPS o SSL (porta 443). Concretamente, i servizi web (Port `80`) vengono reindirizzati alla porta del proxy (in questo caso: `3128`). Qualora vogliate aggiungere altre reti o servizi, dovrete separarli con uno spazio nella riga corrispondente.

```
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"
```

Per inizializzare il firewall e la nuova configurazione, dobbiamo editare una registrazione nel file `/etc/sysconfig/SuSEfirewall2`. La registrazione `START_FW` deve venire impostata su `"yes""`.

Lanciate Squid come descritto nella sezione 33.4 a pagina 584. Grazie ai file di log in `/var/log/squid/access.log` si può verificare se tutto funziona nel modo dovuto.

Per controllare se tutte le porte sono state configurate correttamente, si può eseguire un port scan dell' host – da un qualsiasi computer al di fuori della nostra rete. Solo la porta di servizio web (80) dovrebbe essere aperta. Il port scan si effettua `nmap -O indirizzo IP`.

33.7 cachemgr.cgi

Il cache manager (cachemgr.cgi) è un programma di aiuto CGI per l'emissione di statistiche sulla memoria necessaria dal processo Squid in esecuzione. Al contrario del logging, la cosa facilita l'amministrazione della cache e la visualizzazione di statistiche.

33.7.1 Configurare

Per prima cosa, è necessario un server web funzionante. Per sapere se Apache è già in esecuzione, come utente `root` eseguite `rcapache status`.

Se appare una comunicazione come la seguente:

```
Checking for service httpd: OK
Server uptime: 1 day 18 hours 29 minutes 39 seconds
```

vuol dire che Apache gira sul nostro computer; altrimenti immettete: `rcapache start`. Così Apache viene lanciato con le impostazioni di default di SUSE LINUX. Infine, dobbiamo copiare il file `cachemgr.cgi` dalla directory `/usr/share/doc/packages/squid/scripts/` nella directory `srv/www/cgi-bin` di Apache:

```
cp /usr/share/doc/packages/squid/scripts/cachemgr.cgi /srv/www/cgi-bin/
```

33.7.2 ACL del cache manager in /etc/squid/squid.conf

Le seguenti impostazioni standard sono necessarie per il cache manager:

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
```

Dovrebbero essere contenute le seguenti regole:

```
http_access allow manager localhost
http_access deny manager
```

La prima ACL è la più importante, poiché il cache manager cerca di comunicare con Squid tramite il protocollo cach_object. Le seguenti regole partono dal presupposto che il server web e Squid girino sullo stesso computer. La comunicazione fra il cache manager e Squid origina nel server web e non nel browser. Se quindi il server web si trova su un altro computer, dobbiamo aggiungere appositamente una ACL come nel seguente file esempio 33.2 in questa pagina.

Esempio 33.2: *Regole di accesso*

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl webserver src 192.168.1.7/255.255.255.255 # IP server web
```

Inoltre servono le seguenti regole del file esempio 33.3 in questa pagina.

Esempio 33.3: *Regole di accesso*

```
http_access allow manager localhost
http_access allow manager webserver
http_access deny manager
```

Se vogliamo accedere a più opzioni (p.es. chiudere la cache da remoto o visualizzare altre informazioni sulla cache), possiamo anche configurare una password per il manager; allora servirà una password per configurare la registrazione `cachemgr_passwd` e la lista delle opzioni da visualizzare. Questa lista appare in `/etc/squid/squid.conf` come parte dei commenti delle registrazioni.

Ad ogni modifica del file di configurazione, bisogna riavviare Squid con il comando `rcsquid reload`

33.7.3 Visualizzare le statistiche

Andate alla relativa pagina web, p.es.:`http://webserver.example.org/cgi-bin/cachemgr.cgi`. Premete su 'continue' e fatevi mostrare le diverse statistiche. Nelle FAQ di Squid, `http://www.squid-cache.org/Doc/FAQ/FAQ-9.html` troverete ulteriori informazioni sulle singole registrazioni che vengono emesse dal cache manager.

33.8 SquidGuard

Questo capitolo vuole solo essere una introduzione alla configurazione di SquidGuard e darvi un paio di consigli sul suo impiego. Troverete informazioni più dettagliate sulle pagine web di SquidGuard: `http://www.squidguard.org`

SquidGuard è un filtro libero (GPL), flessibile e velocissimo, che si occupa di reindirizzare determinati contenuti ed è un "PlugIn" preposto ai controlli di accesso per Squid: permette, per una cache Squid, la definizione di una quantità di regole di accesso con diverse restrizioni per diversi gruppi di utenti. Per reindirizzare, SquidGuard utilizza l'interfaccia standard di Squid.

squidGuard può anche venire utilizzato per:

- limitare l'accesso via Internet a determinati server web e/o URL accettati/noti per alcuni utenti.
- negare l'accesso ad alcuni utenti a determinati server web e/o URL.
- negare l'accesso ad URL ad utenti in base a determinate espressioni regolari o termini.
- reindirizzare URL bloccati a una pagina info "intelligente" basata su CGI.
- reindirizzare gli utenti non registrati ad un modulo di registrazione.
- reindirizzare i banner in un GIF vuoto.
- differenti regole di accesso, dipendenti dall'orario, giorno, data, etc.
- differenti regole per i singoli gruppi di utenti.

Né con squidGuard, né con Squid è possibile:

- filtrare/censurare/editare il testo dei documenti
- filtrare/censurare/editare linguaggi di scripting HTML-embedded come JavaScript o VBscript.

Installate il `squidGuard`. Editate il file di configurazione `/etc/squidguard.conf`. Sotto `http://www.squidguard.org/config/` troverete numerosi esempi di configurazione. Più avanti potrete sperimentare con configurazioni più complesse.

Il prossimo passo consiste nel creare una pagina dummy “accesso negato” o, se il client richiede una pagina web proibita, creare una pagina CGI più o meno complessa per reindirizzare Squid. Anche qui vi consigliamo di utilizzare Apache.

Ora dobbiamo comunicare con Squid di impiegare squidGuard. A questo scopo, usiamo nel file `/etc/squid/squid.conf` le seguenti registrazioni:

```
redirect_program /usr/bin/squidGuard
```

Un’altra opzione di nome `redirect_children` configura la quantità dei diversi “redirect”, quindi processi di reindirizzamento in esecuzione sul sistema, in questo caso squidGuard. SquidGuard è abbastanza veloce da elaborare una quantità considerevole di richieste, è veramente veloce: 100.000 richieste in 10 secondi su un Pentium di 500MHz con 5900 domini, 7880 URL, in totale 13780. Perciò consigliamo di non impostare più di 4 processi, poiché attribuzione di questi processi consuma inutilmente tanta memoria.

```
redirect_children 4
```

Per concludere, fate caricare la nuova configurazione di Squid: `rcsquid reload`. Ora potete testare le vostre impostazioni su un browser.

33.9 Creare dei report di cache con Calamaris

Calamaris è uno script Perl che viene usato per creare rapporti sull’ attività della cache in formato ASCII o HTML. Lavora con file di protocolli di accesso propri di Squid. La home page di Calamaris è `http://Calamaris.Cord.de/`. Il programma è semplice da usare, eseguite il login come `root` ed inserite quanto segue: `cat access.log.files | calamaris` ⟨*options*⟩ `> reportfile`. Quando concatenate più file di protocollo, è importante osservare la sequenza cronologica, ovvero prima vengono i file più vecchi. Le diverse opzioni:

-a output di tutti i report disponibili

-w output come HTML report

-l messaggio o un logo nell’intestazione del report.

Nella pagina di manuale di calamaris, `man calamaris`, troverete altre informazioni sulle diverse opzioni.

Un esempio tipico:

```
cat access.log.2 access.log.1 access.log | calamaris -a -w \
> /usr/local/httpd/htdocs/Squid/squidreport.html
```

in tal modo si pone il report nella directory del server web. Apache dovrà visualizzare i report.

Un altro strumento potente per la creazione di rapporti sulla cache è SARG (Squid Analysis Report Generator). Per maggiori informazioni a riguardo, consultate il sito Internet: `http://web.onda.com.br/orso/`

33.10 Ulteriori informazioni su Squid

Visitate la home page di Squid: `http://www.squid-cache.org/`. Qui troverete la "Squid User Guide" e una vasta raccolta di FAQ su Squid.

Il mini HOWTO per un proxing trasparente del pacchetto `howtoenn` lo trovate dopo il processo di installazione sotto: `/usr/share/doc/howto/en/mini/TransparentProxy.gz` Inoltre esistono mailing list per Squid sotto: `squid-users@squid-cache.org`. L'archivio relativo si trova sotto: `http://www.squid-cache.org/mail-archive/squid-users/`.

Parte IV

Amministrazione

Sicurezza in Linux

Mascheramento e firewall assicurano un flusso di dati e scambio di dati monitorato. SSH (Secure Shell) permette di eseguire il log in su host remoti per via di una connessione cifrata. Cifrando dei file o intere partizioni mette a riparo i vostri dati anche nel caso in cui delle persone inautorizzate riuscissero ad accedere al vostro sistema. Il capitolo si conclude trattando la sicurezza di reti Linux.

34.1 Masquerading e firewall

Se utilizzate Linux in un ambiente collegato in rete e dovete distinguere tra settori interni e settori esterni, potete ricorrere alle funzionalità del Linux kernel per l'amministrazione di pacchetti di rete. L'infrastruttura netfilter offre tutti gli strumenti per implementare un sistema Linux come firewall efficace tra le diverse reti. Grazie a iptables – una tabella generica per la definizione di regole – si può stabilire in modo preciso quali pacchetti hanno via libera e quali invece sono da setacciare. SuSEfirewall2 e il rispettivo modulo di YaST semplificano la configurazione del filtra pacchetti.

34.1.1 Filtrare i pacchetti con iptables

Netfilter e iptables sono preposti al filtraggio, alla modifica ed al NAT (*Network Address Translation*) dei pacchetti di rete. I criteri di filtraggio e le azioni conseguenti vengono salvate in cosiddette chain, catene, ed elaborate l'una dopo l'altra quando vi è un pacchetto di rete in entrata. La sequenza o catena delle regole viene salvata in una tabella. Il comando `iptables` elabora queste tabelle e catene di regole.

Linux ha tre tabelle per le diverse funzionalità di un filtra pacchetti:

filter Questa tabella contiene la maggior parte delle regole, dato che qui avviene il *filtraggio dei pacchetti* vero e proprio. Qui sono riportate le regole per l'accettazione (`ACCEPT`) ed il rifiuto (`DROP`) dei pacchetti.

nat Qui viene definita la modifica dell'indirizzo sorgente e di destinazione dei pacchetti: il *mascheramento* utilizzato per la connessione di una piccola rete privata ad Internet, si tratta di una forma particolare di NAT.

mangle Con le regole qui definite si può intervenire sui valori nell'intestazione IP (ad esempio il *Type of Service*).

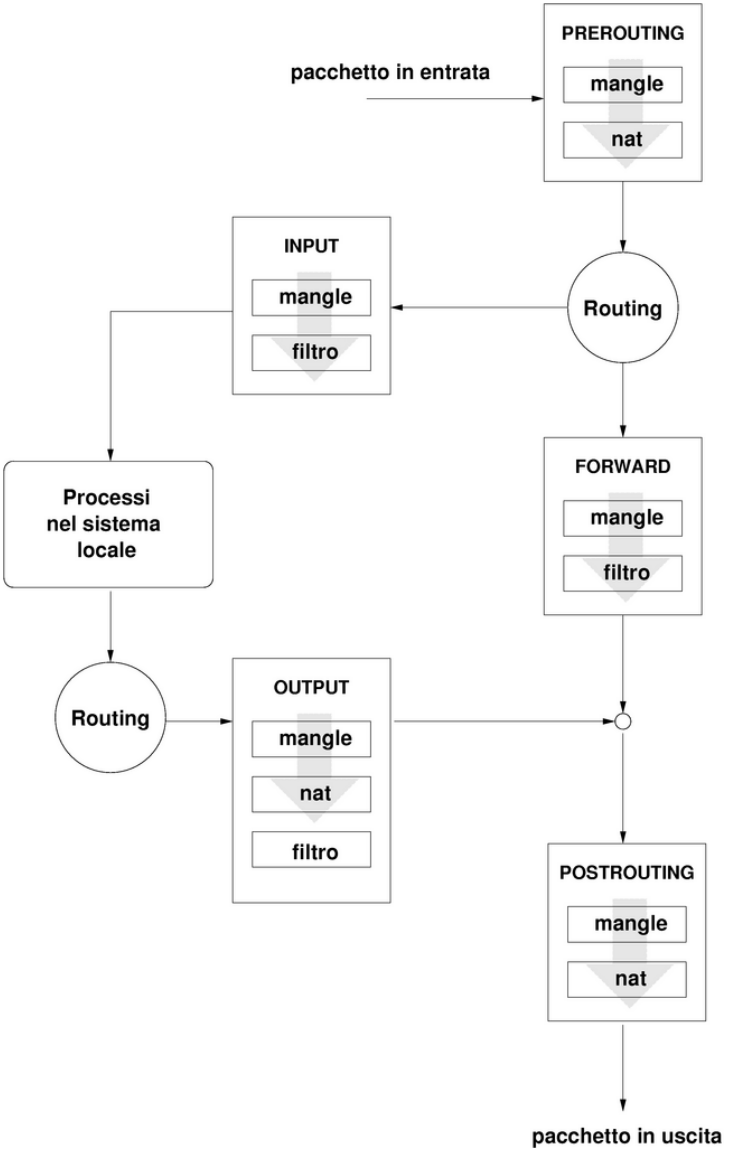

Figura 34.1: *iptables: percorsi possibili di un pacchetto*

Le tabelle menzionate contengono diverse catene di regole predefinite per l'elaborazione dei pacchetti:

PREROUTING Questa catena vale per i pacchetti in entrata.

INPUT Questa catena si occupa dei pacchetti destinati a processi del proprio sistema.

FORWARD Questa catena si occupa dei pacchetti che vengono semplicemente inoltrati.

OUTPUT Questa catena si occupa dei pacchetti che sono stati generati nel proprio sistema.

POSTROUTING Questa catena si occupa di tutti i pacchetti in uscita dal sistema.

La figura 34.1 nella pagina precedente rispecchia il percorso di un pacchetto di rete attraverso il sistema. Per motivi illustrativi le tabelle sono raggruppate in base alle catene, anche se nella realtà sono le catene ad essere raggruppate all'interno delle tabelle.

Nel caso più semplice, un pacchetto raggiunge l'interfaccia `eth0` del sistema ed ha come destinazione il sistema stesso. Innanzitutto il pacchetto viene indirizzato alla catena `PREROUTING` della tabella `mangle`, in seguito viene inoltrato alla catena `PREROUTING` della tabella `nat`. Nel fase successiva viene riconosciuto che il pacchetto è destinato ad un processo del proprio sistema. Dopo aver attraversato le catene `INPUT` delle tabelle `mangle` e `filter` il pacchetto raggiunge la sua destinazione; premesso che le regole di filtraggio definite nella tabella `filter` non lo impediscono.

34.1.2 I principi del masquerading

Masquerading è l'adattamento Linux di NAT (Network Address Translation), cioé "traduzione di indirizzi rete". Questa funzionalità viene applicata quando si tratta di collegare una piccola LAN con indirizzi IP privati (si veda la sezione 22.1.2 a pagina 402) ad Internet con i suoi indirizzi IP ufficiali. Affinché gli host della LAN possano collegarsi ad Internet gli indirizzi privati assumono l'aspetto di indirizzi ufficiali. Questo passaggio viene eseguito dal router, frapposto tra LAN e Internet. Il principio di NAT non è particolarmente complicato: il vostro router dispone di più di un'interfaccia di rete, normalmente una scheda di rete e

una interfaccia per l'Internet. Una di queste interfacce vi collegherà con l'esterno, una o diverse delle altre interfacce collegheranno il vostro computer con gli altri computer nella vostra rete. Nella vostra rete locale avete collegato diversi host alla scheda di rete del router Linux la quale, nel nostro esempio, si chiamerà `eth0`. Gli host nella rete inviano i pacchetti non destinati alla rete interna al router o al gateway di default.

Importante

Maschere di rete uniformi

Quando configurate la vostra rete, fate attenzione alla conformità degli indirizzi broadcast e maschere di rete. Altrimenti la vostra rete non potrà funzionare correttamente, visto che non è possibile un corretto instradamento dei pacchetti di rete.

Importante

Se uno dei computer nella vostra rete invia ora un pacchetto destinato a Internet, il pacchetto arriva al vostro router di default. Il router deve essere configurato in modo da inoltrare i pacchetti. Per ragioni di sicurezza, ciò è impostato di default dall'installazione di SUSE LINUX! Impostate la variabile `IP_FORWARD` che si trova nel file `/etc/sysconfig/sysctl` su `IP_FORWARD=yes`.

Il computer meta del collegamento vede solo il vostro router, non però il computer mittente della vostra rete interna, nascosto dietro il vostro router. Da qui il termine masquerading (mascheramento). L'indirizzo meta del pacchetto risposta è a causa della conversione dell'indirizzo nuovamente il router che deve riconoscere i pacchetti e girare i pacchetti all'host giusto.

Poiché il percorso dei pacchetti entranti dipende dalla tabella di masquerading, non ci sono possibilità di aprire un collegamento dall' esterno verso l'interno: questo collegamento non è previsto nella tabella. Nella tabella, ogni collegamento effettuato ha uno stato ben definito, di modo che i relativi parametri nella tabella non possano venire utilizzati da un secondo collegamento.

Di conseguenza, subentrano delle difficoltà con alcune applicazioni: per esempio ICQ, cucme, IRC (DCC, CTCP), e FTP (nel modo PORT). Netscape, il programma FTP standard e tanti altri utilizzano il modo PASV che con filtra pacchetti e masquerading causa meno difficoltà.

34.1.3 Principi del firewall

Firewall è probabilmente una delle definizioni più diffuse per descrivere un meccanismo che collega fra loro due reti e che provvede ad un traffico di dati moni-

torato. Il metodo che vi presentiamo qui dovrebbe chiamarsi *filtra pacchetti*. Un filtra pacchetti regola il traffico sulla base di criteri come protocollo, porta ed indirizzi IP. In questo modo, siete in grado di settacciare quei pacchetti che, sulla base del loro indirizzo, non possono entrare nella vostra rete. Se ad esempio volete permettere l'accesso al vostro server web, dovete attivare la porta corrispondente. Il contenuto di questi pacchetti non viene controllato finché sono indirizzati in modo corretto (p.es. hanno come meta il vostro server web). Il pacchetto potrebbe quindi attaccare un programma CGl sul vostro server web, senza venir bloccato dal filtro.

Un costrutto più efficace, anche se più complesso, potrebbe essere una combinazione di diversi sistemi, come ad esempio, la combinazione di un filtra pacchetti con l'aggiunta di un gateway/proxy per le applicazioni. Il filtra pacchetti respingerà quei pacchetti che non sono indirizzati alla porta attivata e lascierà passare solo i pacchetti destinati ad un gateway di applicazioni. Questo proxy finge di essere l'interlocutore del server che si vuole collegare con noi. Da questo punto di vista, un tale proxy può essere considerato una macchina di masquerading a livello del protocollo della rispettiva applicazione. Un esempio per un proxy del genere, è Squid, un server proxy http, per il quale dovete configurare il vostro browser in modo che richieste di pagine HTML vengano replicate dalla memoria del proxy e solo se la pagina non viene trovate lì, la richiesta verrà instradata su Internet. La SUSE proxy-suite (il pacchetto `proxy-suite`), contiene un server proxy per il protocollo ftp.

Adesso vogliamo concentrarci sul pacchetto filtra pacchetti di SuSE Linux. Per ulteriori informazioni e link consultate l'HOWTO del firewall contenuto nel `howto`. Se questo pacchetto è stato installato, potete leggerlo con il comando `less /usr/share/doc/howto/en/Firewall-HOWTO.txt.gz`.

34.1.4 SuSEfirewall2

SuSEfirewall2 è uno script che trasforma le variabili configurate in `/etc/sysconfig/SuSEfirewall2` in regole iptables. SuSEfirewall2 presenta tre cosiddette zone di sicurezza (delle quali tratteremo comunque solo le prime due nel seguente esempio di configurazione):

Rete esterna Il sistema va protetto da eventuali attacchi provenienti da una rete esterna, di solito in questi casi si intende l' Internet, ma si può anche intendere altri tipi di rete non protette come ad es. una WLAN.

Rete interne In questi casi si intende la LAN. Se all'interno di questo tipo di rete utilizzate degli indirizzi IP del campo degli indirizzi privato (si veda la sezione 22.1.2 a pagina 402), bisogna ricorrere alla Network Address Translation (NAT), affinché da una rete privata si possa accedere ad una rete esterna.

Zona demilitarizzata (DMZ) Le macchine che si trovano all'interno di una zona demilitarizzata sono indirizzabile sia da una rete esterna che dalla rete interna, non possono però accedere all'Intranet. Questo tipo di configurazione tutela ulteriormente la rete interna da quella esterna, visto che dai sistemi nella DMZ non sarà possibile accedere agli host sulla rete interna.

Ogni traffico di rete non consentito esplicatemente dalla regole viene, bloccato da iptables. Per tale ragione ogni singola l'interfaccia tramite la quale i pacchetti raggiungono la rete deve far capo ad una delle tre zone, e per ogni zona va definito quali servizi e protocolli sono consentiti. Le regole valgono solo per pacchetti che giungono da una rete esterna. I pacchetti creati in locale possono essere inviati comunque.

Potrete eseguire la configurazione ricorrendo ad YaST (si veda la sezione Configurazione con YaST in questa pagina) o direttamente nel file `/etc/sysconfig/SuSEfirewall2` che contiene delle indicazioni in lingua inglese. Alcuni scenari esempio sono riportati inoltre in `/usr/share/doc/SuSEfirewall2/EXAMPLES`.

Configurazione con YaST

Importante

Configurazione automatica del firewall

YaST avvia automaticamente su tutte le interfacce da voi configurate un firewall. La configurazione generata automaticamente viene adatta da YaST tramite le opzioni 'Porte aperte su interfaccia selezionata nel firewall' o 'Porte aperte su firewall' nei moduli sulla configurazione server, non appena viene configurato e abilitato un servizio sul vostro sistema. Se nelle finestre dei moduli server vi è inoltre un bottone 'Dettagli firewall', potete attivare ulteriori servizi e porte. Il modulo di YaST per la configurazione del firewall è stato ideato semplicemente per abilitare o disabilitare il firewall o per eseguire una riconfigurazione del servizio.

Importante

Il processo di configurazione in modalità grafica si avvia tramite il centro di controllo YaST. Selezionate nella categoria 'Sicurezza e utente' → 'Firewall'. La configurazione si suddivide in cinque sezioni:

Avvio Impostate il comportamento all'avvio in questa finestra. Di default SuSEfirewall2 gira in un sistema appena installato. Qui potete anche lancare e fermare il Firewall here. Se volete testare le attuali impostazioni del firewall, utilizzate il pulsante 'Salva impostazioni e riavvia il firewalla ora.'

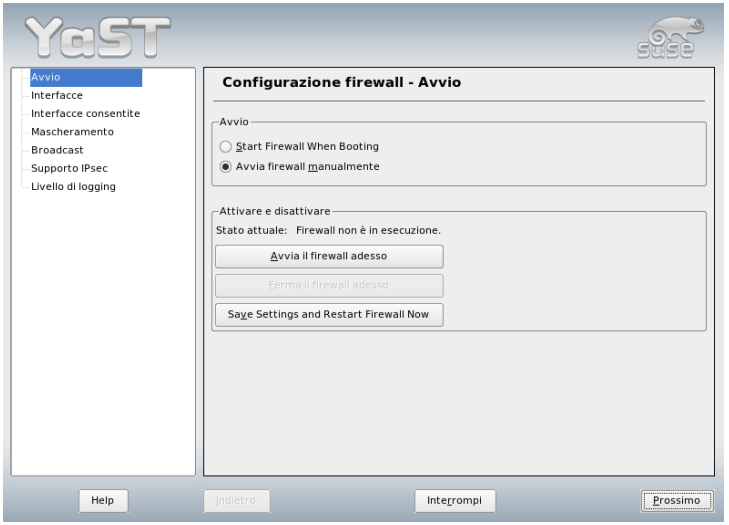

Figura 34.2: *YaST: configurazione del firewall*

Interfacce Tutte le interfacce di rete rilevate sono qui elencate. Per rimuovere un'interfaccia da una zona, selezionate l'interfaccia premete su 'Modifica' e selezionate '____no_zone____'. Se volete aggiungere un'interfaccia ad una zona, selezionate l'interfaccia e premete su 'Modifica' e selezionate una delle zone disponibili. Potete anche creare un'interfaccia speciale con le vostre impostazioni ricorrendo a 'Personalizzato'.

Interfacce consentite Questa opzione vi permette di offrire dei servizi ad una zona protetta. Di default, solo la zona esterna è protetta. In questo caso dovete indicare esplicitamente i servizi visibili agli host esterni. Abilitate

il rispettivo servizio dopo aver selezionata la zona in 'Servizio consentito per zona selezionata'.

Mascheramento Il mascheramento vi permette di nascondere la vostra rete interna nei confronti di rete esterne, tipo Internet. Consente di accedere in modo trasparente alla rete esterna. Le richieste provenienti dalla rete esterna indirizzate alla rete interna vengono bloccate, mentre le richieste della rete interna, dall'esterno, sembrano provenire dal server di mascheramento.

Se dei servizi particolari di una macchina interna devono essere resi disponbili ad una rete esterna, vanno specificati delle regole di reindirizzamento per il servizio in questione.

Broadcast In questa finestra, vengono configurate le porte UDP che consentono dei broadcast. I numeri delle porte o i servizi richiesti devono essere separati da una spazio. Si veda inoltre il file `/etc/services`.

Il logging di broadcast non consentiti può essere abilitato qui. Ciò può essere accompagnato da difficoltà, poiché host Windows utilizzano dei broadcast per conoscersi a vicenda e quindi generano una quantità considerevole di pacchetti non consentiti.

Supporto IPsec In questa finestra potete impostare se i servizi IPsec saranno. Sotto 'Dettagli' potete indicare i pacchetti fidati.

Livello di logging Vi sono due tipi di logging: pacchetti consentiti e pacchetti non consentiti. Quelli consentiti vengono ACCEPTED, ossia accettati, quelli non consentiti DROPPED o REJECTED, ossia rifiutati. Potete scegliere tra 'Protocolla tutto', 'Protocolla pacchetti cruciali' o 'Non protocollare niente' per entrambi.

Una volta completata la configurazione del firewall, uscite dalla finestra tramite 'Prossimo'. Vedrete le impostazioni del firewall relative alle zone che potrete modificare. Tutti i servizi, tutte le porte e protocolli consentiti vengono elencati in questo sommario. Se volete tornare alla configurazione, utilizzate 'Indietro', altrimenti premete 'Accetto' per salvare la vostra configurazione.

Configurazione manuale

In questa sezione illustreremo come procedere nella configurazione. Di volta in volta indicheremo se quanto detto vale per il mascheramento o per il firewall. Nel file di configurazione sono illustrati gli aspetti riguardanti una DMZ ("Zona

demilitarizzata"), quindi in questa sete non entreremo nei dettagli. Queste zone demilitarizzate si propongono per reti aziendali.

Abilitate innazitutto tramite il modulo YaST Editor dei runlevel il SuSEfirewall2 per il vostro runlevel (probabilmente 3 o 5). Verranno creati dei link simbolici per gli script SuSEfirewall2_* nelle directory `/etc/init.d/rc?.d/`.

`FW_DEV_EXT` (Firewall, mascheramento)
L'interfaccia connessa a Internet. Per modem utilizzate `ppp0`, per ISDN `ipppo`, per DSL `dsl0`; con `auto` utilizzate l'interfaccia della route di default.

`FW_DEV_INT` (Firewall, mascheramento)
Indicate l'interfaccia connessa alla rete interna, "privata" (ad esempio `eth0`). In assenza di una rete interna lasciate vuota questa variabile ed le impostazioni firewall interesseranno solo l'host su cui gira.

`FW_ROUTE` (Firewall, mascheramento)
Se vi serve il mascheramento, impostate questa variabile su `yes`. I vostri host interni non saranno visibili dall'esterno, dal momento che hanno indirizzi di rete privati (p.es. `192.168.x.x`) che non verranno instradati (routed) su Internet.

Per un firewall senza mascheramento selezionate qui `yes`, solo se volete permettere l'accesso alla rete interna. Per fare questo i computer interni devono avere indirizzi IP ufficiali. Di solito però, *non* dovreste consentire l'accesso ai vostri sistemi dall'esterno!

`FW_MASQUERADE` (Mascheramento) Se intendete fare uso del mascheramento, immettete qui `yes`. Tenete presente che è più sicuro se gli host della rete interna accedono ad Internet tramite il server proxy.

`FW_MASQ_NETS` (Mascheramento) Indicate qui gli host o reti da mascherare. Lasciate uno spazio tra le singole voci. Esempio:

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

`FW_PROTECT_FROM_INTERNAL` (Firewall)
Immettete qui `yes`, se volete proteggere il firewall anche da attacchi dall'interno. In questo caso, dovrete esplicitamente attivare i servizi disponibili per la rete interna. Si veda anche `FW_SERVICES_INT_TCP` e `FW_SERVICES_INT_UDP`.

FW_AUTOPROTECT_SERVICES (Firewall)
Di solito si lascia su `yes` per la creazione automatica di regole esplicite da applicare ai servizi in esecuzione.

FW_SERVICES_EXT_TCP (Firewall) Inserite qui le porte TCP a quali accedere per una semplice postazione di lavoro domestica che non debba offrire alcun servizio, di solito si lascierà vuota.

FW_SERVICES_EXT_UDP (Firewall) Lasciate vuoto questo campo, a meno che non stiate usando un server dei nomi a cui si deve accedere dall'esterno. Altrimenti inserite qui le porte UDP richieste.

FW_SERVICES_INT_TCP (Firewall) Qui stabilite i servizi disponibili per la rete interna. Le indicazioni sono analoghe a quelle in `FW_SERVICES_EXTERNAL_TCP`, solo che si riferiscono in questo caso alla rete *interna*. Questa variabile va configurata solo avete abilitato `FW_PROTECT_FROM_INT`.

FW_SERVICES_INT_UDP (Firewall) Si veda FW_SERVICES_INT_TCP.

A questo punto avete concluso il processo configurativo. Non dimenticate di testare il firewall. Come utente `root` invocate `SuSEfirewall2 start`. Tramite ad esempio un `telnet` dall'esterno potete vedere se questo collegamento venga effettivamente respinto; in questo caso dovreste avere in `/var/log/messages` un output del genere:

```
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)
```

Anche i pacchetti nmap o nessus consentono di testare le impostazioni del firewall. La documentazione su nmap è reperibile sotto `/usr/share/doc/packages/nmap` e la documentazione su nessus nella directory `/usr/share/doc/packages/nessus-core`, chiaramento dopo aver installato i rispettivi pacchetti.

34.1.5 Ulteriori informazioni

La documentazione aggiornata per il pacchetto `SuSEfirewall2` è reperibile sotto `/usr/share/doc/packages/SuSEfirewall2`. La home page del progetto

netfilter e iptables, `http://www.netfilter.org`, offre tanta documentazione tradotta in varie lingue.

34.2 SSH: lavorare in tutta sicurezza su host remoti

Lavorare in rete spesso comporta dover accedere ad host remoti. L'utente deve autenticarsi tramite il proprio nome di login e password. Se questi dati non vengono cifrati possono venir intercettati da terzi e utilizzati per eseguire il login all'insaputa dell'utente. A parte il fatto che in tal modo verrebbe violata la privacy dell'utente, l'intrusore può utilizzare l'accesso per sferrare degli attacchi contro altri sistemi oppure conferirsi i diritti dell'amministratore o dell'utente `root` del relativo sistema. In passato per collegare due host remoti si usava Telnet sprovvisto di qualsiasi meccanismo di cifratura o di sicurezza contro tentativi di intrusione; offrono poca sicurezza anche i semplici collegamenti FTP o alcuni programmi che permettono di copiare dei dati da un host all'altro.

Il software SSH offre la protezione necessaria. Le stringhe di autenticazione, di solito il nome utente e la password, ed anche il processo di comunicazione avvengono in forma cifrata; anche qui è possibile intercettare dei dati trasmessi ma senza la chiave di cifratura non è possibile decifrare il flusso di dati. Quindi si realizza una comunicazione sicura attraverso una rete insicura come Internet. SUSE LINUX offre il pacchetto OpenSSH.

34.2.1 Il pacchetto OpenSSH

Con SUSE LINUX viene installato di default il pacchetto OpenSSH. Avrete a vostra disposizione i programmi ssh, scp e sftp, come alternativa a telnet, rlogin, rsh, rcp e ftp. Nella configurazione di default, si potrà accedere ad un sistema SUSE LINUX solo tramite utility OpenSSH e solo se il firewall consente l'accesso.

34.2.2 Il programma ssh

Con il programma ssh, potete stabilire un collegamento ad un sistema remoto e lavorarci interattivamente. Questo programma sostituisce quindi sia telnet che rlogin. Il programma slogin è solo un link simbolico che rimanda a ssh. Per fare

un esempio: con il comando `ssh sole`, si può accedere al sistema sole che vi chiederà la vostra password.

Dopo l'autenticazione, potrete lavorare sia dalla riga di comando che interattivamente, p.es. con YaST. Se il nome utente locale e quello sul sistema remoto differiscono, potete indicare un nome differente p.es. `ssh -l augusto sole` o `ssh augusto@sole`.

Inoltre, ssh offre la possibilità, già nota in rsh, di eseguire dei comandi su un altro sistema. Nel seguente esempio, viene eseguito il comando `uptime` su sole e creata una directory con il nome `tmp`. L'output del programma viene visualizzato sul terminale locale del sistema terra.

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

Le virgolette servono qui per riunire le due istruzioni in un comando; solo così verrà eseguito anche il secondo comando sul sistema sole.

34.2.3 scp – copiare in modo sicuro

Per mezzo di scp potete copiare dei file su un host remoto. scp è il sostituto cifrato e sicuro di rcp. Per esempio, `scp miotesto.tex sole:` copia il file `miotesto.tex` dal sistema terra sul sistema sole. Se il nome utente su terra differisce da quello su sole, potete impostare quest'ultimo con `nomeutente@nomehost`. Non esiste un'opzione `-l` per questo comando.

Dopo aver immesso la password, scp inizia con la trasmissione dei dati e ne indica lo stato di avanzamento con una barra formata da asterischi che cresce da sinistra a destra. Inoltre, sul margine destro viene mostrato il tempo rimanente (stimato) per la trasmissione (ingl. estimated time of arrival). Ogni output può venire soppresso con l'opzione `-q`.

scp consente non solo di copiare singoli file ma offre anche una funzionalità di copiatura ricorsiva per poter copiare intere directory: `scp -r src/ sole:backup/` copia l'intero contenuto della directory `src/` sottodirectory incluse su sole e lì nella sottodirectory `backup/`. Se questa sottodirectory non dovesse ancora esistere, viene generata automaticamente.

Per mezzo dell'opzione `-p`, scp non modifica la datazione dei file. `-C` provvede ad una trasmissione compressa. In questo modo, viene ridotto al minimo il volume dei dati da trasmettere, anche se questo processo comporta un considerevole carico di lavoro per il processore.

34.2.4 sftp - trasmissione più sicura

Al posto di scp si può usare sftp. Una sessione sftp offre molti dei comandi noti di ftp. Rispetto a scp si rivela vantaggioso soprattutto quando si trasmettono dati di cui si ignorano i nomi dei file.

34.2.5 Il demone SSH (sshd): lato server

Affinché possano venire utilizzati i programmi client del pacchetto SSH, ossia ssh e scp, un server, in questo caso il demone di SSH, deve girare in sottofondo, e mettersi in ascolto su `TCP/IP port 22`. Durante il primo avvio, il demone genera tre paia di chiavi composte da una parte privata e da una pubblica. Per questo si usa definire questo approccio come procedimento basato su chiave pubblica. Per garantire una comunicazione sicura tramite SSH, solo l'amministratore deve poter accedere ai file delle chiavi private. A questo scopo, i permessi dei file vengono impostati (preimpostati) in modo molto restrittivo durante l'installazione di default. Le chiavi private sono richiese localmente solo dal demone SSH e non devono venir trasmesse a nessun altro. Le chiavi pubbliche (riconoscibili dall'estensione `.pub`), invece, vengono trasmesse al client che chiede di collegarsi e sono quindi leggibili per tutti gli utenti.

Il client SSH cerca di stabilire una connessione. Il demone SSH in attesa e il client SSH richiedente scambiamo i dati di identificazione per confrontare la versione di protocollo e di software ed escludere la connessione ad una porta errata. Dato che è un processo figlio del demone SSH a replicare, sono possibili una serie di connessioni SSH contemporanee.

OpenSSH supporta ai fini della comunicazione tra server SSH e client SSH il protocollo SSH nella versione 1 e 2. Se eseguite una nuova installazione di SUSE LINUX verrà installato automaticamente la versione 2 del protocollo. Se dopo un aggiornamento volete continuare ad utilizzare SSH 1, seguite le istruzioni riportate in `/usr/share/doc/packages/openssh/README.SuSE`. Lì viene anche descritto come convertire in pochi passaggi un ambiente SSH 1 in un ambiente SSH 2.

Con il protocollo SSH versione 1, il server inivia la sua chiave host (ingl. host key) pubblica ed una chiave server (ingl. server key) che viene rigenerata dal demone di SSH ogni ora. Per mezzo delle due chiavi, il client SSH crea una chiave di sessione (ingl.session key) cifrata e la invia al server SSH. Il client ssh comunica inoltre al server quale metodo di cifratura utilizzare (ingl. cipher).

Il protocollo SSH versione 2 non prevede l'uso della chiave server, ricorre invece all'algoritmo secondo Diffie-Hellman per lo scambio delle chiavi.

Le chiavi host e server private, assolutamente necessarie per decifrare la chiave di sessione, non possono venire dedotte dalle chiavi pubbliche. In questo modo, solo il demone SSH contattato è in grado di decifrare la chiave di sessione grazie alla sua chiave privata (si veda `man /usr/share/doc/packages/openssh/RFC.nroff`). Questa fase iniziale del collegamento si lascia seguire da vicino ricorrendo all'opzione `-v` preposta alla ricerca di errori (debugging).

Di default viene utilizzato il protocollo SSH versione 2; con il parametro `-1` potete tuttavia forzare l'uso della versione 1 del protocollo SSH. Il client archivia tutte le chiavi host pubbliche in `~/.ssh/known_hosts` dopo la prima presa di contatto con l'host remoto. In tal modo è possibile respingere tentativi di attacchi del tipo man-in-the-middle con server SSH che utilizzano nomi ed indirizzi IP contraffatti. Questi tentativi verranno smascherati a causa di una chiave host non inclusa in `~/.ssh/known_hosts` oppure vista l'impossibilità del server di decifrare la chiave di sessione dal momento che manca la controparte privata.

É consigliabile archiviare su di un supporto esterno ed in un luogo sicuro le chiavi private e pubbliche di `/etc/ssh/`. In questo modo, accertate eventuali manipolazione delle chiavi, potrete ripristinare le vecchie chiavi reinstallandole. Così risparmiate agli utenti l'avvertimenti pochi rassicuranti. Una volta accertato che, nonostante l'avviso, si tratta del server SSH giusto, eliminate la registrazione relativa a questo sistema da `~/.ssh/known_hosts`.

34.2.6 Meccanismi di autenticazione SSH

Ora segue l'autenticazione vera e propria, che, nella variante più semplice prevede l'immissione di una password, così come negli esempi sopra citati. Con SSH si è voluto introdurre un software sicuro e al contempo facile da usare, con un metodo di autenticazione semplice come quello dei programmi che intende sostituire (rsh e rlogin). Con SSH vi è un ulteriore paio di chiavi generato dall'utente. A questo scopo il pacchetto SSH contiene il tool ssh-keygen. Immettendo `ssh-keygen -t rsa` o `ssh-keygen -t dsa` viene generato il paio di chiavi e vi verrà chiesto il nome del file nel quale archiviare le chiavi:

Confermate il valore di default e indicate la passphrase. Anche se il software vi consiglia di non indicare una passphrase, consigliamo di inserire comunque una stringa lunga da 10 a 30 caratteri. Non utilizzate parole o frasi semplici o brevi. Il programma vi chiederà di inserire la frase una seconda volta. Infine, vi mostrerà dove le chiavi pubbliche e private siano state archiviate, ovvero, nel nostro esempio, nei file `id_rsa` e `id_rsa.pub`.

Usate `ssh-keygen -p -t rsa` o rispettivamente `ssh-keygen -p -t dsa` per modificare la vostra passphrase. Copiate la parte pubblica della chiave (nel nostro esempio `id_rsa.pub`) sul sistema remoto, dove la salvate sotto `~/.ssh/authorized_keys`. Ogni volta che vi connetterete, vi verrà chiesta la passphrase. In caso contrario, verificate la locazione ed il contenuto dei file summenzionati.

A lungo andare, questo procedimento è più laborioso dell'inserimento di una password. Quindi, il pacchetto SSH fornisce un altro tool: ssh-agent che tiene pronte le chiavi private per la durata di una X session; a questo scopo, l'intera X session viene avviata come processo figlio di ssh-agent. Potete realizzare ciò semplicemente impostando la variabile `usessh` all'inizio del file `.xsession` su `yes`, ed eseguire il login tramite un display manager (p.es.KDM o XDM). Alternativamente potete usare `ssh-agent startx`.

Ora potete utilizzare `ssh` o `scp`. Se avete distribuito la vostra chiave pubblica come descritto sopra, non dovreste più ricevere la richiesta d'inserimento della password. Quando uscite dal vostro sistema, fate attenzione a terminare la vostra X session o a non permettere a nessuno di accedervi ad es. impostando una applicazione per bloccare lo schermo protetta da una password, p.es. xlock.

Tutte le principali modifiche con l'introduzione della seconda versione del protocollo SSH, sono riportate nel file `/usr/share/doc/packages/openssh/README.SuSE`.

34.2.7 X: inoltro e autenticazione

Oltre ai miglioramenti in termini di sicurezza finora descritti, ssh facilita anche l'uso di applicazioni X remote. Se inserite `ssh` con l'opzione `-X`, sul sistema remoto viene automaticamente impostata la variabile DISPLAY e tutte le emissioni di X vengono reindirizzate, tramite il collegamento ssh, sul sistema di partenza. Questa comoda funzione previene contemporaneamente la possibilità d'intercettazione esistente finora nelle applicazioni X lanciate su un sistema remoto e con visualizzazione sul sistema locale.

Tramite l'opzione `-A`, viene il meccanismo di autenticazione di ssh-agent viene passato al prossimo sistema. In tal modo è possibile passare da un sistema all'altro senza dover inserire una password; questo però solo se prima sono state distribuite e archiviate correttamente le chiavi pubbliche sui sistema meta interessati.

Per precauzione, entrambi i meccanismi non sono attivi di default. Per attivarli permanentemente, andate nel file di configurazione del sistema, `/etc/ssh/ssh_config` o in quello dell'utente `~/.ssh/config`.

Potete utilizzare ssh anche per reindirizzare un collegamento TCP/IP. Come esempio riportiamo l'inoltro della porta SMTP e POP3:

```
ssh -L 25:sole:25 terra
```

Con questo comando ogni collegamento indirizzato a *terra port 25* (SMTP) viene reindirizzato alla porta SMTP di sole tramite un canale cifrato. Ciò è utile specialmente per gli utenti di server SMTP senza supporto per le funzionalità SMTP-AUTH o POP-before-SMTP. Le e-mail possono in tal maniera venir inviate da una postazione qualsiasi con un collegamento di rete per essere consegnate al proprio server di posta (ingl."home" mail server). In modo analogo con il seguente comando le richieste POP3 (porta 110) di terra possono essere inoltrate alla porta POP3 di sole.

```
ssh -L 110:sole:110 terra
```

Questi comandi vanno eseguiti come utente `root`, poiché vengono indirizzate porte locali privilegiate. Con un collegamento SSH esistente, la posta viene spedita e ritirata da utente normale. L'host SMTP e l'host POP3 deve venire configurato su `localhost`. Per ulteriori informazioni consultate le pagine di manuale dei singoli programmi e dei file sotto `/usr/share/doc/packages/openssh`.

34.3 Cifrare delle partizioni e file

34.3.1 Campi di applicazione

Ogni utente ha dei dati sensibili che non dovrebbero essere accessibili a terzi. Se lavorate in ambienti di rete o con dispositivi mobili dovreste porre particolare attenzione a questo aspetto. Si consiglia di cifrare dei file o partizioni intere quando sono anche altre persone a poter accedere al vostro sistema sia fisicamente che tramite una connessione di rete. Ecco dei scenari in cui è consigliabile cifrare file e partizioni:

Notebook Utilizzate preferibilmente un dispositivo mobile per il vostro lavoro e sul vostro notebook avete salvato dei dati sensibili? Cifrate le relative partizioni del disco rigido. Se smarrite il vostro notebook oppure anche in caso di furto i vostri dati sono al sicuro da accessi non autorizzati grazie ad una partizione cifrata o in un singolo file cifrato.

Supporti estraibili Chiavi USB o dischi rigidi esterni sono esposti a dei furti nella stessa maniera dei notebook. Un file system cifrato tutela i vostri dati.

34.3.2 Configurazione con YaST

YaST vi permette di cifrare file o partizioni già durante il processo di installazione che in un momento qualsiasi successivo a sistema installato. Un file cifrato si lascia generare in ogni momento, dal momento che si integra senza difficoltà alcuna nello schema di partizionamento dato; una partizione cifrata deve essere impostata come una partizione a sé stante. Il partizionamento standard proposto da YaST non prevede dello spazio da dedicare ad una partizione cifrata. Quindi dovrete modificare lo schema di partizionamento manualmente per creare una partizione cifrata.

Impostare una partizione cifrata durante l'installazione

Avvertimento

Immissione della password

All'immissione della password leggete attentamente gli avvisi riguardanti la sicurezza della password, e tenetela ben in mente. Se dimenticate la password non vi sarà possibile accedere ai vostri dati cifrati.

Avvertimento

Nella finestra YaST per esperti riferita al partizionamento ('Preparare il disco rigido: modo per esperti'), che viene illustrato nella sezione 2.7.5 a pagina 73, selezionate 'Crea', come per una partizione normale, per impostare una partizione cifrata. Nella finestra successiva, in cui impostate i parametri di partizionamento, stabilite il tipo di formattazione ed il punto di mount della nuova partizione e cliccate su 'Cifrare file system'. Nella finestra successiva immettete la password da utilizzare due volte per motivi di sicurezza. Non appena uscite dalla finestra di partizionamento con 'OK', viene generata la nuova partizione cifrata. Al prossimo boot del sistema dovrete immettere la password prima di eseguire il mount della partizione cifrata. Se il primo tentativo dovesse fallire, la password vi verrà richiesta un'altra volta.

Se non volete che al boot venga eseguito il mount della partizione cifrata lasciate vuota la richiesta di password. Rispondete con "No" alla seguente domanda se intendete immettere nuovamente la password. In questo caso il vostro file system cifrato non verrà montato ed il resto del sistema viene avviato come di consueto. Il mount automatico di una partizione cifrata rende in parte vano il concetto di sicurezza che ne sta alla base, dato che la partizione, una volta concluso il processo

di avviamento del sistema, sarà a disposizione di tutti gli utenti, se non viene eseguito immediatamente l'unmount dopo l'accesso. Quindi questa opzione è sensata solo volete tutelare i vostri dati da un eventuale furto del vostro dispositivo mobile sul quale lavorate esclusivamente voi da soli ed il dispositivo al momento del furto era spento.

Se non volete immettere la password ad ogni boot del sistema e intendete montare la partizione cifrata solo all'occorrenza, selezionate nella finestra 'Opzioni fstab' l'opzione 'Non montare al boot del sistema'. Per accedervi dovrete montarla esplicitamente con: `mount` ⟨*`nome_partizione`*⟩ ⟨*`punto_di_mount`*⟩. Dopo aver immesso la password viene eseguito il mount della partizione che sarà quindi a vostra disposizione. Dopodiché eseguite: `umount nome_partizione` per escludere che un altro utente possa accedervi.

Impostare una partizione cifrata con il sistema in esecuzione

Avvertimento

Abilitare la cifratura con il sistema in esecuzione

Quanto descritto per la fase di installazione vale anche per l'impostazione di una partizione cifrata con il sistema in esecuzione. Tenete comunque presente che se cifrate una partizione già esistente, cancellate tutti i dati in essa contenuti.

Avvertimento

Se il vostro sistema è in esecuzione avviate il modulo 'Partizionamento' tramite il menu 'Sistema' del centro di controllo di YaST. Rispondete con 'Sì' alla domanda di sicurezza riferita al partizionamento di un sistema in esecuzione per ottenere una panoramica delle partizioni disponibili. Invece di selezionare 'Crea' come descritto sopra, fate clic su 'Modifica'. Il modo di procedere è uguale a quello descritto sopra. E come descritto sopra potrete stabilire se la partizione debba essere montata automaticamente al boot o esplicitamente all'occorrenza.

Impostare file cifrati

Sussiste inoltre la possibilità di creare dei file system cifrati che si basano su file per tutelare i vostri dati sensibili. Il punto di partenza è rappresentato come per le partizioni cifrate dalla finestra di 'Preparare il disco rigido: modo per esperti'. Selezionate 'file cifrato' e nella finestra successiva indicate il percorso del file. Inoltre stabilite lo spazio da dedicare a questo tipo di file. Accettate le impostazioni

predefinite per la formattazione e file system. Infine stabilire se e dove il file system debba venir montato all'avvio del sistema o se intendete eseguirne il mount e l'unmount in modo a sé stante.

File cifrati presentano il vantaggio che possono essere aggiunti senza dovere intervenire sul partizionamento del disco rigido. Esse vengono montate tramite un loop device e si comportano come comuni partizioni.

Cifrare dei file tramite l'editor vi

Utilizzare partizioni cifrate presentano lo svantaggio che finché è montata, almeno l'utente `root`– può accedere ai dati. Per evitare ciò, potete utilizzare il vi nel modo cifrato.

Utilizzate `vi -x nomefile` per editare un nuovo file. vi chiederà l'immissione della password e quindi cifra il contenuto del file. Ad ogni accesso il vi chiederà la password.

Per essere davvero sicuri, potreste anche salvare un file cifrato su una partizione cifrata. Questo è indicato anche per il fatto che il meccanismo di cifratura del vi non spicca per robustezza.

34.3.3 Cifrare il contenuto di supporti estraibili

Dischi rigidi esterni o chiavi USB vengono rilevati da YaST alla stregua di dischi rigidi per così dire normali. Se volete cifrare file o partizioni su dispositivi del genere, procedete come descritto sopra. Tra le 'Opzioni fstab' selezionate assolutamente l'opzione 'Non montare al boot del sistema', dato che supporti del genere solitamente non sono disponibili all'avvio del sistema, ma vengono connessi con il sistema già in esecuzione.

34.4 La sicurezza è una questione di fiducia

Una delle principali caratteristiche di un sistema Linux/Unix è quella di consentire a diversi utenti di lavorare contemporaneamente sul medesimo sistema (multi user e multitasking). Il sistema operativo offre inoltre trasparenza per quel che riguarda la rete, di modo che gli utenti spesso non sanno se i file o le applicazioni con cui lavorano si trovano sul computer locale o se vi accedono tramite la rete.

Per permettere a più utenti di lavorare su un sistema, i loro dati devono poter essere gestiti separatamente. E' anche una questione di sicurezza e tutela della privacy. La sicurezza dei dati era indispensabile già quando i computer non erano ancora collegati in rete. Ogni volta che veniva a mancare un supporto dati (di solito un disco rigido) o quando veniva danneggiato, si doveva pur continuare a poter accedere ai dati più importanti, anche se tali danni significavano, allora, l'interruzione temporanea dell'attiva di enormi infrastrutture.

Anche se questo capitolo si concentra sulla segretezza dei dati e la tutela della privacy degli utenti, vogliamo tuttavia sottolineare che un buon concetto di sicurezza sottintende sempre un regolare backup funzionante e aggiornato. Senza il backup, non solo sarà difficile accedere ai dati sul disco in caso di un difetto dell'hardware, ma il backup é anche importante in particolar modo se vi è il sospetto che qualcuno abbia rovistato e magari manipolato in modo non autorizzato i nostri dati.

34.4.1 Sicurezza locale e sicurezza della rete

Vi sono diversi modi per accedere ai dati:

- parlando con qualcuno che disponga delle informazioni che si vorrebbero avere o che abbia accesso a determinati dati di un computer,
- direttamente dalla console di un computer (accesso fisico),
- tramite un cavo seriale oppure
- tramite rete.

In tutti questi casi, dovrebbe esserci una costante: prima di ottenere l' accesso ai dati o alle risorse, l'utente dovrebbe autenticarsi. Per un server web chiaramente le cose cambiano, comunque sicuramente non volete che il vostro server web riveli a un navigatore qualsiasi i vostri dati privati.

Il primo caso dell' elenco sopraccitato è il più comune tra tutti: in banca, p.es., dovete dimostrare all'impiegato di essere la persona alla quale è permesso l'accesso ad un determinato deposito, con la vostra firma, un codice PIN o una password. In alcuni casi, si possono menzionare determinati fatti noti o usare la retorica per guadagnare la fiducia della persona in possesso delle informazioni e farne rivelare alcune, a volte senza che la vittima se ne renda neanche conto. Gli hacker chiamano questo comportamento *social engineering*. Contro questo tipo di attacco,

l'unica difesa è esserne cosciente. Accessi illeciti su computer spesso sono preceduti da una presa di contatto del tipo social engineering con il personale di una ditta, fornitore di servizi o anche con dei componenti della famiglia; purtroppo, spesso ce se ne accorge quando ormai è troppo tardi.

Chi vuole accedere (in modo non autorizzato) a dei dati, ha anche la possibilità di servirsi dello strumento più tradizionale: l'hardware. Infatti, anche l'hardware è esposto a questo tipo di attacchi. Il computer deve essere protetto dal prelievo, scambio o sabotaggio di parti o dell'intero sistema (compreso naturalmente il backup) - questo vale anche per il cavo di rete o di alimentazione. Il procedimento di avvio deve essere sicuro: infatti, le combinazioni di tasti più comuni possono causare determinate reazioni del computer. In questo caso, ci si aiuta anche con l'uso di password per l'accesso al BIOS e al boot loader.

Terminali seriali connessi a interfacce seriali sono ancora molto diffusi. Per la trasmissione di caratteri in chiaro viene usato un semplice cavo (o un' interfaccia ad infrarossi). In questo caso, il cavo stesso è il punto vulnerabile: è sufficiente collegarvi una vecchia stampante per registrare il flusso di dati. Quello che è possibile con una stampante, è possibile anche con altri mezzi più sofisticati.

Dal momento che l'apertura in locale di file su di un computer sottosta a restrizioni di natura diversa rispetto all'accesso via rete ad un server remoto, bisogna distinguere tra sicurezza locale e sicurezza di rete. La linea di demarcazione è rappresentata dal luogo in cui i dati vengono assemblati in pacchetti per poter essere trasmessi e raggiungere l' applicazione sull'altro host.

Sicurezza locale

Come già accennato, la sicurezza locale comincia con la localizzazione fisica del computer. Noi partiamo dal presupposto che il vostro computer sia ubicato in modo da soddisfare i vostri criteri di sicurezza. In tema di sicurezza locale si tratta in prima linea di distinguere tra i singoli utenti, in modo che nessun utente possa assumere i permessi o l'identità di un altro utente. Questo vale in generale e in particolare nel caso dei permessi di `root`, dal momento che l' utente `root` è, nel sistema, una presenza onnipotente, in grado di diventare ogni utente locale e di leggere ogni file locale.

Le password

Linux non memorizza le password in chiaro ovvero in forma non cifrata e non confronta la password immessa con quella archiviata. Altrimenti, tutti gli account del sistema sarebbero compromessi non appena qualcuno non autorizzato riuscisse ad accedere al file in questione. Linux salva quindi le password in forma

cifrata, ogni volta che immettete la vostra password, questa viene cifrata e solo allora paragonata con quella archiviata. Un procedimento del genere funziona solo se non è possibile evincere la password vera e propria dalla forma cifrata.

A tal fine vi sono dei cosiddetti algoritmi non invertibili che funzionano solo in una direzione, detti anche algoritmi *trapdoor*. Un aggressore che sia riuscito ad impadronirsi della password cifrata non potrà ricavare semplicemente la password applicando nuovamente lo stesso algoritmo. Per ottenere la password in chiaro dovrebbe provare tutte le combinazioni di lettere possibili, finchè non trovi quella che coincide con la vostra password. Considerando che ogni password può constare anche di otto lettere, le combinazioni possibili sono fin troppe...

Negli anni '70, un argomento a favore della sicurezza di questo metodo era la lentezza dell'algoritmo che richiedeva alcuni secondi per cifrare una password. I computer moderni però sono in grado di eseguire fino a milioni di crittogrammi al secondo. Per questo motivo, le password non dovrebbero essere visibili per ogni utente (`/etc/shadow` non è leggibile per l'utente normale) e le password non dovrebbero essere facili da indovinare – per il caso che, a causa di un errore, le password diventino visibili. Camuffare una password come "Fantasia" usando "F@nt@s13" non è molto d'aiuto.

Queste regole di scambio sono un gioco facile per certi programmi che si servono anche di dizionari per indovinare la password. La cosa migliore sono combinazioni di lettere che, messe assieme, non formano alcuna parola sensata e che hanno un significato solo per voi (ad esempio, le iniziali delle parole di una frase o del titolo di un libro, come "Il Nome della Rosa" di Umberto Eco, che risulterebbe in una bella password: "INdRdUE9"). Per indovinare una password come "Inter" o "Robi76", poi, non c'è neanche bisogno di conoscervi a fondo.

Il processo di caricamento

Non consentite il caricamento daI dischetto o dal CD-ROM rimuovendo i lettori o impostando una password per l'accesso al BIOS e configurate il BIOS in modo da consentire il boot esclusivamente dal disco rigido. Generalmente, i sistemi Linux vengono inizializzati con un boot loader che permette di passare opzioni supplementari al kernel da avviare. Per quel che riguarda la sicurezza, tali opzioni sono molto critiche, quindi impostate un'ulteriore password in `/boot/grub/menu.lst` (si veda il capitolo 8 a pagina 177) per evitare che chiunque possa passare delle opzioni al processo di boot. Anche perchè il kernel non funziona solo con diritti `root`, ma assegna fin dall'inizio i diritti `root`.

Permessi di accesso

Qui vale il principio: lavorare sempre con i minori privilegi possibili. Non è assolutamente necessario leggere o scrivere una e- mail come `root`. Se il programma e-mail ha un bug, la gravità delle conseguenze per voi dipenderà dai permessi con i quali lavoravate al momento dell'attacco. Qui si tratta quindi di limitare quanto più possibile i danni.

I singoli permessi dei più 200.000 file di una distribuzione SUSE sono stati assegnati in modo molto oculato. L'amministratore di un sistema dovrebbe installare software o file supplementari solo con la massima cautela e fare particolarmente attenzione all'assegnazione dei permessi dei file. Amministratori esperti e coscienziosi, quando usano il comando `ls`, aggiungono sempre l'opzione `-l` per avere un elenco dettagliato dei file assieme ai permessi di accesso in modo da poter riconoscere subito diritti impostati erroneamente. Un attributo impostato in modo errato può significare non solo che i file potrebbero venire sovrascritti o cancellati, ma anche che i file modificati potrebbero venire eseguiti da `root` o che i file di configurazione possano essere utilizzati con permessi di `root`. In questo modo l'aggressore avrebbe la possibilità di estendere notevolmente il suo raggio di azione. Questo tipo di attacchi vengono chiamati "uova del cuccù", perchè il programma (l'uovo) viene eseguito (covato) da un utente estraneo (l'uccello): proprio come il cuccù, che fa covare le sue uova da altri uccelli.

Un sistema SUSE LINUX include i file `permissions`, `permissions.easy`, `permissions.secure` e `permissions.paranoid` che si trovano nella directory `/etc`. Qui vengono stabiliti i permessi particolari come p.es. directory con accesso in scrittura per tutti (world writable) o setuser-ID-bit per file, cioé il programma non viene eseguito coi permessi del proprietario del processo che lo ha iniziato, ma coi permessi del proprietario del file che è generalmente `root`. L'amministratore ha a disposizione il file `/etc/permissions.local` in cui poter apportare le proprie modifiche.

La scelta del file da usare per l'assegnazione dei permessi nel caso di programmi di configurazione SUSE, si lascia eseguire comodamente selezionando 'Sicurezza' in YaST. Per ulteriori informazioni leggete i commenti in `/etc/permissions` e la pagina di manuale del comando `chmod` (`man chmod`).

Overflow del buffer e i format string bug

Ogni qualvolta un programma elabora dei dati che possono essere modificati da un utente è sempre bene essere prudenti. Questa prudenza vale soprattutto per il programmatore dell' applicazione: questi deve assicurare che i dati vengano

interpretati correttamente dal programma e che non vengano scritti in aree della memoria troppo piccole. Inoltre dovrà essere garantito che i dati vengano elaborati in modo consistente.

Si ha un *buffer overflow* quando si scrive in un'area del buffer, senza badare alla dimensione effettiva del buffer. Potrebbe essere che i dati (generati dall'utente) abbiano bisogno di più spazio di quello disponibile nel buffer: a causa di questo sforamento dei limiti del buffer, succede che un programma dovendo elaborare dei dati dell'utente, esegua sequenze di programmi che si trovano sotto la sfera di influenza dell'utente e non del programmatore. Questo è un grave errore, specialmente se il programma viene eseguito con diritti speciali (si veda la sezione Permessi di accesso a fronte).

I *format string bug* funzionano un po' diversamente, ma anche questi utilizzano le immissioni dell'utente per sviare il programma. Questi errori di programmazione di solito vengono sfruttati da programmi eseguiti con privilegi speciali, cioè programmi setuid e setgid. Potete quindi proteggere il vostro sistema e voi stessi da tali errori, togliendo dai programmi i rispettivi permessi di esecuzione. Anche qui vale il principio dei minori permessi possibili (si veda la sezione Permessi di accesso nella pagina precedente).

Poiché i buffer overflow e format string bug sono degli errori che interessano l'elaborazione dei dati degli utenti, questo tipo di bug può essere sfruttato non solo se si dispone già di un login locale: molti degli errori conosciuti possono venire sfruttati anche tramite un collegamento di rete. Quindi, buffer overflow e format string bug non si lasciano classificare nettamente come attinenti esclusivamente alla sicurezza locale o alla sicurezza della rete.

Virus

Esistono virus anche per Linux! I virus conosciuti sono stati scritti come *proof of concept*, ovvero per verificare il funzionamento del programma. Ma finora non ne è ancora stato avvistato nessuno in libera circolazione.

Per diffondersi, i virus hanno bisogno di un ospite, senza non possono sopravvivere. Questo ospite può essere un programma o una parte importante della memoria (per il sistema), come ad es. il master boot record, ed essere sovrascrivibile dal codice di programma del virus. Grazie alle sue capacità multi user, Linux offre la possibilità di limitare l'accesso in scrittura ai file, in particolar modo ai file sistema. Se lavorate come `root`, aumentate la possibilità che il vostro sistema venga contagiato da un virus. Se, invece, vi attenete alla regola dei minori privilegi possibili, sarà difficile contagiare il vostro sistema Linux con un virus.

Inoltre, non dovreste mai eseguire sconsideratamente un programma preso da Internet di cui ignorate l'origine. I pacchetti rpm della SUSE portano una firma cifrata; questa firma digitale è la garanzia per l'accuratezza del modo in cui sono stati assemblati i pacchetti SUSE. Virus sono una prova del fatto che anche un sistema che presenta un elevato grado di sicurezza diventa vulnerabile quando l'amministratore o l'utente opera in modo sconsiderato per quando riguarda la sicurezza.

I virus vanno distinti dai cosiddetti vermi informatici che interessano la sicurezza delle reti e non richiedono un sistema ospite per proliferare.

Sicurezza della rete

Per quando riguarda la sicurezza della rete l'intero sistema va protetto contro attacchi provenienti dall'esterno. L'autenticazione dell'utente durante il login attraverso nome di login e password sono parte del concetto della sicurezza locale. Nel caso di login tramite una connessione di rete bisogna distinguere tra due aspetti di sicurezza: fino all'autenticazione si parla di sicurezza di rete, ad autenticazione avvenuta di sicurezza locale.

X Windows (autenticazione X11)

Come già accennato, la trasparenza di rete è un caratteristica fondamentale di un sistema UNIX; questo vale particolarmente per X, il sistema di windowing dei sistemi UNIX. Esso consente ad es. di eseguire il login su un computer remoto ed inizializzare lì un programma che verrà visualizzato tramite la rete sul vostro computer.

Per visualizzare da remoto un X client utilizzando un X server, il server dovrà proteggere le risorse che amministra (il display) da accessi non autorizzati. Concretamente significa che al programma del client devono essere assegnati determinati permessi. Su X Windows, questo avviene in due modi: controllo degli accessi basato su host e controllo degli accessi basato su cookie. Il primo caso si basa sull'indirizzo IP del computer sul quale deve girare il programma del client e viene controllato con il programma xhost. Il programma xhost amministra un indirizzo IP di un client autorizzato in una mini-banca dati che si trova sull'X server. Basare l'autenticazione esclusivamente su un indirizzo IP non è però molto sicuro. Sul computer, con il programma client, potrebbe essere attivo un secondo utente e questi avrebbe accesso all'X server esattamente come qualcuno che rubi l'indirizzo IP. A causa di questo inconveniente non vogliamo approfondire tale metodo di autenticazione. La pagina di manuale di `xhost` vi fornirà maggiori dettagli che potrete consultare eseguendo `man xhost`.

Con l'accesso di controllo basato sui cookie viene generata una stringa di caratteri nota solo al X server ed all'utente loggato correttamente. Al login, questi cookies (con questa parola, si intendono i fortune cookies cinesi contenenti una massima o un detto) vengono memorizzati nel file `.Xauthority` nella directory home dell'utente ed è disponibile in questo modo per ogni client X Windows che vuole visualizzare una finestra sul X server. Il programma `xauth` mette a disposizione dell'utente il tool per analizzare il file `.Xauthority`. Se cancellate `.Xauthority` dalla vostra directory home o lo rinominate, non potrete più aprire delle nuove finestre o X client. Nella pagina di manuale di `Xsecurity` (`man Xsecurity`) troverete maggiori informazioni sugli aspetti riguardanti la sicurezza di X Windows.

ssh (secure shell) consente di cifrare un collegamento di rete all' X server in modo trasparente per l'utente; in questi casi si parla di X forwarding. Sul lato server, viene simulato un X-server e sull'host remoto viene impostata la variabile DISPLAY per la shell. Per maggiori dettagli su SSH si veda la sezione 34.2 a pagina 614.

Avvertimento

Se siete del parere che il computer sul quale fate il login non sia sicuro, non utilizzate l'X forwarding. Con l'X11 forwarding attivato, un aggressore potrebbe collegarsi al vostro X server tramite il collegamento SSH e intercettare le vostre immissioni di tastiera (ingl. sniffing).

Avvertimento

Buffer overflow e format string bugs

Come già accennato nella sezione Overflow del buffer e i format string bug a pagina 626, buffer overflow e format string interessano sia la sicurezza locale che della rete. Come per la variante locale dei bug, ossia errori di programmazione, i buffer overflow nelle applicazione di rete, se sfruttati con successo, permettono quasi sempre di ottenere i permessi di `root`. Anche se l'aggressore non arriva a tanto, può comunque procurarsi l'accesso ad un account locale (non privilegiato) tramite cui sfruttare altre falle nella sicurezza del sistema (locale).

I buffer overflow e format string bug sono indubbiamente le varianti più frequenti di un attacco sferrato da remoto. Nelle mailing list sulla sicurezza, sono reperibili i cosiddetti exploits, programmi cioé che sfruttano lacune rilevate di recente. Anche chi non conosce i dettagli esatti di questa lacuna, è in grado di sfruttarla. Con il passare degli anni si è appurato che la libera disponibilità degli exploit

codes ha contribuito a rendere i sistemi operativi più sicuri; la cosa dipende sicuramente anche dal fatto che i produttori di sistemi operativi sono costretti ad eliminare i bug del loro software. Poichè con il software libero, il codice sorgente è a disposizione di tutti (SUSE LINUX fornisce tutti i sorgenti disponibili), ognuno che rileva una lacuna con un exploit code può anche fare proposte su come risolvere il problema.

DoS - Denial of Service

L'obiettivo di questo tipo di attacco è bloccare un servizio o addirittura l'intero sistema. Ciò può succedere nei modi più disparati: creare un sovraccarico del sistema bombardandolo con pacchetti insensati o sfruttando un remote buffer overflow. Una volta bloccato un dato servizio, il processo di comunicazione è esposto ad un attacco cosiddetto *man-in-the-middle* (sniffing, tcp connection hijacking, spoofing) e DNS poisoning.

man in the middle: sniffing, tcp connection hijacking, spoofing

Un attacco dalla rete, nel quale l'aggressore si posiziona tra due interlocutori, viene chiamato attacco del tipo man-in-the-middle. Spesso la vittima neanche se ne accorge. Ecco uno dei tanti scenari possibili: l'aggressore intercetta una richiesta di collegamento e la inoltra al sistema meta. La vittima, senza saperlo, si è collegata ad un host sbagliato, visto che questi si spaccia per il computer meta.

L'attacco man in the middle più semplice è rappresentato da uno *sniffer*. L'aggressore spia i collegamenti di rete che gli passano davanti (ingl. sniffing, cioè spiare). La cosa diventa più complessa, se l'aggressore nel mezzo cerca di rapire (ingl. hijacking) un collegamento già esistente. Per poter predire i numeri di sequenza TCP esatti del collegamento, l'aggressore deve analizzare per un pò di tempo i pacchetti. Quando assume il ruolo della meta del collegamento, la vittima lo nota solo perchè il collegamento viene terminato perché non valido.

L'aggressore sfrutta soprattutto quei protocolli non cifrati che non offrono protezione contro l'hijacking e che eseguono una autenticazione semplice all'inizio del collegamento.

Per *spoofing* si intende l'invio di pacchetti con i dati di origine modificati, di solito l'indirizzo IP. Quasi tutte le varianti di attacco richiedono l'invio di pacchetti falsificati; cosa che sotto Linux/UNIX può venire eseguita solo dal superutente (`root`).

Molte delle varianti di attacco menzionati vengono eseguite in combinazione con un DoS. Se all'aggressore è data la possibilità di bloccare un computer (anche se

solo per breve tempo), la cosa gli agevola l'ulteriore decorso dell'attacco visto che l'host in questione non potrà interferire per un certo lasso di tempo.

DNS poisoning

In questo caso l'aggressore utilizza pacchetti di risposta DNS falsificati (spoofed) per corrompere la cache di un server DNS, con lo scopo di far inviare al server certi dati a chi, la vittima, si rivolge al server con delle richieste. Per indurre il server DNS ad accettare le informazioni, l'aggressore analizza alcuni pacchetti del server. Molti server classificano determinati host, sulla base del loro indirizzo IP e del loro nome host, come affidabili. Un attacco del genere presume che l'aggressore disponga di buona conoscenza del rapporto di fiducia instaurato per poter fingere di essere uno degli host affidabili e fidati. L'aggressore spesso deve sferrare anche un attacco contro il server dei nomi. Per evitare tutto questo si consiglia di utilizzare una collegamento cifrato che permette di verificare l'identità del sistema meta del collegamento.

Vermi informatici

I vermi vengono spesso confusi coi virus. Vi è tuttavia una notevole differenza tra i due: un verme non deve contagiare alcun programma ospite ed è tagliato per diffondersi rapidamente nella rete. Noti vermi come Ramen, Lion o Adore sfruttano lacune di sicurezza ben conosciute di programmi di server come bind8 o lprNG. E' relativamente semplice proteggersi dai vermi, perchè di solito trascorrono pochi giorni dalla comparizione di un verme che sfrutta determinate falle e la disponibilità dei pacchetti di aggiornamento. Ciò presuppone, naturalmente, che l'amministratore installi tutti i più recenti security update.

34.4.2 Consigli e trucchetti: indicazioni generali

Informazione: in tema di sicurezza è necessario tenere il passo con gli sviluppi nel campo dell'informatica ed essere sempre al corrente sulle novità dei più recenti problemi di sicurezza. Una buona protezione contro gli errori di tutti i tipi è l' immediata installazione dei pacchetti di update annunciati raccomandati da un security announcement. Gli annunci di sicurezza di SUSE vengono divulgati per mezzo di una mailing list nella quale potete registravi sotto `http://www.novell.com/linux/security/securitysupport.html`. La mailing list `suse-security-announce@suse.de` è la prima fonte di informazione per i pacchetti update che viene aggiornata da parte di membri del security team di SUSE

La mailing list `suse-security@suse.de` è un foro di discussione molto informativo per il campo della sicurezza. Potete registrarvi a questa lista tramite la stessa URL indicata per `suse-security-announce@suse.de`.

Una delle mailing list dedicata alla sicurezza più conosciuta al mondo è `bugtraq@securityfocus.com` che consigliamo vivamente. Su `http://www.securityfocus.com` troverete ulteriori informazioni.

Ecco alcune utili regole di base in tema di sicurezza:

- Lavorate il meno possibile come `root`, secondo il principio: per ogni compito, servitevi dei minori privilegi possibili. Diminuirete così non solo il pericolo che si infiltrino uova di cuccù e virus ma anche la possibilità di causare voi stessi degli errori irreparabili.
- Se possibile, utilizzate sempre collegamenti cifrati per eseguire dei lavori da remoto. `ssh` (secure shell) dovrebbe essere utilizzato al posto di `telnet`, `ftp`, `rsh` e `rlogin`
- Non usate alcun metodo di autenticazione che si basi solo sull' indirizzo IP.
- Tenete sempre aggiornati i vostri pacchetti principali per la rete ed abbonatevi alle mailing list per gli update dei software (p.es. bind, sendmail, ssh). Lo stesso vale per software rilevante solo per la sicurezza locale.
- Ottimizzate i permessi di accesso ai file critici in termini di sicurezza: fatelo intervenendo sul file `/etc/permissions`. Se rimuovete il setuid bit da un programma, forse non sarà in grado di assolvere al suo compito, ma almeno non rappresenta più un rischio per la sicurezza. Idem per i world writable file e le world writable directory, ovvero file e directory a cui possono accedere tutti in scrittura.
- Disattivate ogni servizio di rete non strettamente necessario sul vostro server. Ciò rende sicuro il vostro sistema. Con il programma `netstat`, potete rilevare porte aperte (con lo stato socket LISTEN). Come opzioni possono venire usate `netstat -ap` o `netstat -anp`. Con l'opzione `-p` vedete quale processo occupa con quale nome quale porta.

  Confrontate il risultato di un port scan del vostro sistema eseguito dall'esterno con quello di netstat; a questo scopo si adatta particolarmente il programma nmap che controlla ogni singola porta e, sulla base della risposta del vostro computer, è in grado di trarre conclusioni riguardanti il servizio disponibile dietro una determinata porta. Non eseguite mai uno port scan senza il permesso esplicito dell'amministratore addetto, poichè

la cosa potrebbe venire scambiata per un tentativo di attacco. Ricordate di eseguire un port scan non solo delle porte TCP, ma anche delle porte UDP (opzioni `-sS` e `-sU`).

- Per un controllo affidabile dell'integrità dei file del vostro sistema, dovreste utilizzare `tripwire`. Cifrate la banca dati generata da `tripwire` per proteggerla da manipolazioni. In ogni caso avete anche bisogno di un backup ovvero copia di sicurezza di questa banca dati su un supporto dati a parte a cui non è possibile accedere tramite rete.

- Fate attenzione quando installate del software. Si sono già verificati dei casi in cui un aggressore ha incluso in archivi tar di software di sicurezza un cavallo di Troia. Per fortuna ci si è accorti subito. Se installate un pacchetto binario, controllate la provenienza del pacchetto.

  I pacchetti rpm SUSE portano una firma gpg. La chiave utilizzata da SUSE per firmare è

  ID:9C800ACA 2000-10-19 SuSE Package Signing Key <build@suse.de>

  Key fingerprint = 79C1 79B2 E1C8 20C1 890F 9994 A84E DAE8 9C80 0ACA

  Il comando `rpm --checksig package.rpm` mostra se la somma di controllo e la firma del pacchetto da installare sono esatte. La chiave si trova sul primo CD o DVD della distribuzione e sulla maggioranza dei key-server nel mondo.

- Controllate regolarmente il backup dei dati e del sistema. Un backup corrotto non ha valore alcuno.

- Controllate i vostri file di log. Se possibile, scrivetevi un semplice script che rilevi delle registrazioni sospette nei vostri file di log. Questo è un compito tutt'altro che triviale, poichè solo voi sapete cosa è strano o cosa non lo è.

- Utilizzate `tcp_wrapper` per limitare l'accesso ai singoli servizi del vostro computer a quegli indirizzi IP a cui è esplicitamente permesso l'accesso. Nella pagine di manuale di tcpd e `hosts_access` (`8 tcpd`, `man hosts_access`) troverete ulteriori informazioni su `tcp_wrapper`.

- In aggiunta a tcpd (tcp_wrapper) potreste usare il SuSEfirewall per incrementare ulteriormente il livello di sicurezza.

- Meglio esagerare in questi casi: ricordate che è meglio ricevere una comunicazione due volte che non ricerverla proprio.

34.4.3 Rivelazione di nuovi problemi di sicurezza

Se individuate delle lacune nella sicurezza del sistema (controllate i pacchetti di update disponibili), rivolgetevi all'indirizzo e-mail `security@suse.de`. Inviate un'esatta descrizione del problema assieme al numero della versione del pacchetto usato. Cercheremo di rispondervi il più presto possibile. Se possibile, cifrate la vostra e-mail con pgp. La chiave pgp di SUSE è:

```
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
```

Potrete scaricare la chiave anche all'indirizzo `http://www.novell.com/linux/security/securitysupport.html`.

35

Le Access Control List in Linux

Questo capitolo introduce brevemente i principi e il modo di funzionare di POSIX ACL per file system Linux. Vi indicheremo come espandere il sistema dei permessi tradizionale per file e directory tramite le ACL (*Access Control List*) e tratteremo i vantaggi che ne derivano.

L'espressione *POSIX ACL* suggerisce che si tratta di un vero standard POSIX (*Portable Operating System Interface*). Per una serie di motivi le relative bozze standard POSIX 1003.1e e POSIX 1003.2c sono state ritirate, però tanti sistemi operativi UNIX si basano su questi documenti. L'implementazione descritta in questo capitolo delle ACL per file system si attiene a quanto esposto in questi documenti che trovate alla seguente URL: `http://wt.xpilot.org/publications/posix.1e/`

35.1 Vantaggi delle ACL

Di solito per ogni file o directory in Linux vi sono tre tipi di permessi, ovvero di lettura (`r`), di scrittura (`w`) ed il permesso di esecuzione (`x`) per le tre categorie di utenti: proprietario (ingl. owner), gruppo proprietario (ingl. group) ed altri (ingl. other) o "il resto del mondo". Inoltre, in casi speciali vi è la possibilità di impostare il *set user id*, il *set group id* e lo *sticky* bit. Per la maggior parte dei casi che si verificano nella prassi quotidiana questo modello snello è più che sufficiente. Per scenari più complessi o applicazioni più avanzate, gli amministratori di sistema hanno dovuto escogitare una serie di espedienti per aggirare le restrizioni insite nel modello dei permessi tradizionale.

In quei casi in cui il modello dei permessi tradizionale deve essere esteso entrano in gioco le ACL. Esse permettono di assegnare dei permessi a singoli utenti o gruppi, anche diversi dal proprietario o dal gruppo del proprietario.

Le ACL sono una caratteristica del kernel di Linux e al momento vengono supportate da ReiserFS, Ext2, Ext3, JFS e XFS. Grazie alle ACL è possibile realizzare dei scenari di una certa complessità senza dover intervenire al livello della applicazione per implementare complessi modelli di permessi di accesso.

Quando si sostituisce un server Windows con uno Linux si apprezzeranno i vantaggi offerti dalle ACL. Alcune delle postazioni di lavoro potranno continuare a girare su Windows anche a migrazione avvenuta. Il server Linux offrirà ai client Windows servizi di gestione file e di stampa tramite Samba. Visto che Samba supporta le ACL, i permessi degli utenti si lasciano impostare sia sul server Linux che tramite un'interfaccia grafica Windows (solamente Windows NT e successivi). winbindd permette addirittura di concedere agli utenti senza un account sul server Linux dei permessi che esistono solo in Windows.

35.2 Definizioni

Categorie di utenti Il tradizionale modello dei permessi POSIX conosce tre *categorie* di utenti per l'assegnazione di determinati permessi: il proprietario (ingl. owner), il gruppo proprietario (ingl. group) e gli altri utenti o anche "il resto del mondo" (ingl. other). Per ogni categoria di utenti possono essere concessi rispettivamente i tre bit dei permessi (ingl. permission bits) per l'accesso in lettura (`r`), l'accesso in scrittura (`w`) ed il permesso di esecuzione (`x`).

ACL di accesso I permessi di accesso degli utenti e gruppi per file o directory vengono stabiliti tramite ACL di accesso (ingl. access ACL).

ACL di default Le ACL di default valgono solo per le directory e determinano quali permessi un oggetto del file system, al momento della sua creazione, eredita dalla directory superiore.

ACL entry Ogni ACL è composta da una serie di ACL entry ovvero registrazioni ACL. Una registrazione ACL include il tipo (si veda la tabella 35.1 nella pagina seguente), una designazione per l'utente o il gruppo a cui si riferisce la registrazione ed i permessi. Per alcuni tipi di registrazione non si inserisce la designazione del gruppo o dell'utente.

35.3 Utilizzare le ACL

tabella 35.1 nella pagina successiva riassume i sei diversi tipi di registrazioni ACL disponibili, ciascuna definisce i permessi per un utente o un gruppo di utenti. La registrazione di tipo *owner* (proprietario) definisce i permessi per l'utente che possiede il file o la directory. La registrazione *owning group* (gruppo proprietario) definisce i permessi del gruppo a cui il file appartiene. L'amministratore di sistema (ingl. superuser) può modificare il proprietario o il gruppo di appartenenza del file con i comandi `chown` o `chgrp`. Ogni registrazione *named user* (utente designato) definisce i permessi dell'utente inserito nel campo qualificatore della registrazione, che è il campo intermedio nel modulo mostrato in tabella 35.1 nella pagina seguente. Ogni registrazione *named group* (gruppo designato) definisce i permessi del gruppo inserito nel campo qualificatore della registrazione. Solo per i *named user* e i *named group* il campo qualificatore della registrazione non è vuoto. La registrazione *other* (altri) definisce i permessi per tutti gli altri utenti.

La registrazione *mask* limita ulteriormente i permessi assegnati alle registrazioni *named user*, *named group*, e *owning group* definendo esattamente quali permessi sono attivi e quali sono mascherati. I permessi sono attivi solo se esistono in una delle registrazioni elencate e se sono presenti nella maschera. Se i permessi sono presenti solo nella maschera o solo nella registrazione corrente, non sono attivi e quindi i permessi non sono concessi. Tutti i permessi definiti nelle registrazioni *owner* e *owning group* sono sempre attivi. L'esempio in tabella 35.2 in questa pagina fornisce una dimostrazione di questo meccanismo.

Le ACL si possono suddividere in due categorie. L'ACL *minima* è composta esclusivamente da registrazioni del tipo *owner* (proprietario), *owning group* (gruppo proprietario) ed *other* (altri) e corrisponde ai tradizionali bit dei permessi per file e directory. Le ACL *estese* (ingl. extended) vanno oltre. Esse devono contenere una registrazione *mask* (maschera) e possono contenere diverse registrazioni del tipo *named user* e *named group*.

Tabella 35.1: *Tipi di registrazione ACL*

Tipo	**Formato**
owner	`user::rwx`
named user	`user:name:rwx`
owning group	`group::rwx`
named group	`group:name:rwx`
mask	`mask::rwx`
other	`other::rwx`

Tabella 35.2: *Mascheramento dei permessi di accesso*

Tipo	**Forma del testo**	**Permessi**
named user	`user:geeko:r-x`	`r-x`
mask	`mask::rw-`	`rw-`
	Permessi effettivi:	`r--`

35.3.1 Le registrazioni ACL ed i bit dei permessi

Le due figure illustrano il caso di una ACL minima e di una estesa (si veda la figura 35.1 in questa pagina e figura 35.2 in questa pagina). Vedete tre blocchi. A sinistra si ha l'indicazione del tipo della registrazione ACL, in centro una ACL esempio e a destra i corrispondenti bit dei permessi secondo il modello dei permessi tradizionale, come visualizzato anche dal comando `ls -l`. In entrambi i casi i permessi *owner class* vengono associati alla registrazione ACL *owner*. Si ripete anche l'attribuzione dei permessi *other class* alla registrazione ACL corrispondente. L'attribuzione dei permessi *group class* cambia invece nei due casi.

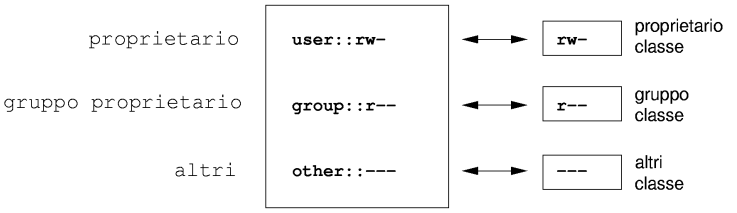

Figura 35.1: *ACL minima: registrazioni ACL vs. bit dei permessi*

Nel caso di una ACL minima — ovvero senza registrazione *mask* — i permessi *group class* vengono assegnati alla voce ACL *owning group* (si veda la figura 35.1 in questa pagina). Nel caso di ACL estese — dunque con la registrazione *mask* — i permessi *group class* vengono assegnati alla voce *mask* (si veda la figura 35.2 in questa pagina).

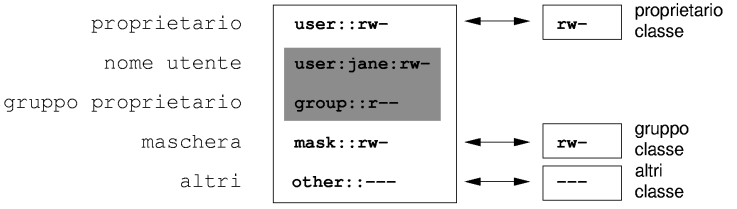

Figura 35.2: *ACL estese: registrazioni ACL vs. bit dei permessi*

Grazie a questo tipo di assegnazione viene garantito che le applicazioni con e

senza supporto per le ACL possano interagire senza difficoltà alcuna. I permessi di accesso che sono stati stabiliti tramite i bit dei permessi rappresentano il limite massimo per le "impostazioni mirate" effettuate tramite le ACL. Tutti i permessi non riportati, o non sono stati impostati nella ACL o non sono effettivi. Se si apportano delle modifiche ai bit dei permessi questo si riflette chiaramente anche nelle corrispondenti ACL e viceversa.

35.3.2 Una directory con ACL di accesso

L'esempio seguente fornisce una dimostrazione di come gestire l'accesso con le ACL:

Prima di creare una directory, il comando `umask` vi permette di stabilire a priori quali diritti di accesso mascherare. Con il comando `umask 027` il proprietario mantiene tutti i permessi (`0`, al gruppo non viene concesso l'accesso in lettura (`2`). Tutti gli altri utenti non hanno nessun permesso di accesso (`7`). Per avere maggiori informazioni su `umask`, consultate la relativa pagina di manuale (`man umask`).

Con il comando `mkdir mydir` viene creata la directory `mydir` con i permessi stabiliti con `umask`. Usate il comando `ls -dl mydir` per controllare se i permessi sono stati assegnati correttamente. L'output del comando per questo esempio dovrebbe essere:

```
drwxr-x--- ... tux project3 ... mydir
```

Con il comando `getfacl mydir` potete controllare lo stato iniziale della ACL, le informazioni riportate dovrebbero assomigliare a:

```
# file: mydir
# owner: tux
# group: project3
user::rwx
group::r-x
other::---
```

L'output di `getfacl` rispecchia esattamente la correlazione tra i bit dei permessi e le registrazioni ACL descritta nella sezione 35.3.1 nella pagina precedente. Nelle prime tre righe dell'output si ha il nome, il proprietario e il relativo gruppo della directory. Le successive tre righe indicano le tre registrazioni ACL *owner*, *owning group* ed *other*. Complessivamente per quanto riguarda le ACL (minime) il

comando `getfacl` non emette alcuna informazione che non fosse emessa anche dal comando `ls`.

Il vostro primo intervento sulle ACL mira a concedere ad un ulteriore utente `geeko` ed ad un ulteriore gruppo `mascots` i permessi di lettura, scrittura ed esecuzione.

```
setfacl -m user:geeko:rwx,group:mascots:rwx mydir
```

Con l'opzione `-m` istruite `setfacl` a modificare le ACL esistenti. Il seguente argomento indica le registrazioni ACL da modificare (se si tratta di diverse registrazioni, esse vanno separata da virgole). Infine indicate il nome della directory per la quale applicare la modifica.

Fatevi mostrare adesso l'ACL immettendo `getfacl`.

```
# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx
group::r-x
group:mascots:rwx
mask::rwx
other::---
```

Oltre alle immissioni fatte da voi per l'utente `geeko` ed il gruppo `mascots` è stata aggiunta una voce *mask*. *mask* viene aggiunto automaticamente per avere un comune minimo denominatore per tutte le registrazioni in *group class*. Inoltre `setfacl` adatta automaticamente le registrazioni in *mask* se modificate delle impostazioni, a meno che non vogliate disabilitare questa funzione con `-n`. *mask* stabilisce il limite massimo dei permessi di accesso valido per tutte le voci all'interno di *group class*, ovvero *named user*, *named group* ed *owning group*. I bit dei permessi di *group class* che verrebbero emessi dal comando `ls -dl mydir` corrispondono ora alla voce `mask`.

```
drwxrwx---+ ... tux project3 ... mydir
```

L'output adesso contiene anche un segno + nella prima colonna, il segno per una ACL *estesa*.

In accordo con l'output del comando `ls` i permessi per la voce *mask* includono anche l'accesso in scrittura. Secondo il modello tradizionale dei permessi di accesso questi bit d'autorizzazione indicherebbero che l'*owning group* (in questo caso: `project3`) ha anche l'accesso in scrittura per la directory `mydir`. Comunque i permessi di accesso veramente validi per l'*owning group* vengono determinati dall'intersezione dei diritti impostati per l' *owning group* e *mask*; dunque nel nostro esempio `r-x` (si veda la tabella 35.2 a pagina 638). In questo caso anche dopo aver aggiunto le registrazioni delle ACL non è cambiato nulla per quel che riguarda i permessi dell' *owning group*.

Con `setfacl` o `chmod` potete apportare delle modifiche a *mask*. Per esempio: usate `chmod g-w mydir`. Il comando `ls -dl mydir` adesso mostra:

```
drwxr-x---+ ... tux project3 ... mydir
```

Il comando `getfacl mydir` produce il seguente output:

```
# 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::---
```

Dopo aver sottratto l'accesso in scrittura al *group class* con `chmod`, l'output del comando `ls` vi fa notare che tramite `chmod` i bit di *mask* sono stati adattati di conseguenza. Ciò risulta più evidente dall'output di `getfacl` che aggiunge dei commenti ad ogni registrazione i cui bit dei permessi effettivamente validi non concordano con quelli impostati originariamente, perché eliminati dalla registrazione *mask*. Naturalmente potrete ripristinare lo stato originario in ogni momento con il relativo comando di `chmod g+w mydir`

35.3.3 Una directory con ACL di default

Per le directory vi sono delle ACL particolari: le ACL di default, con cui stabilire quali permessi di accesso erediterranno, al momento della loro creazione, tutti i sotto-oggetti, cioè le sottodirectory di questa directory. La ACL di default vale sia per le sottodirectory che per i file.

Gli effetti di una ACL di default

Ci sono due modi in cui i permessi di accesso di una ACL di default applicata a una directory vengono trasmessi alle sotto directory e ai file contenuti:

- Una sottodirectory eredita l'ACL di default della directory superiore sia come propria ACl di default che ACL di accesso.
- Un file eredita l'ACL di default come propria ACL di accesso.

Tutte le chiamate di sistema (system calls) per la creazione di oggetti di file system utilizzano un parametro `mode`. Questo parametro `mode` imposta i permessi di accesso per il file o la directory da creare. Se la directory superiore non ha una ACL di default, i permessi risulteranno dall'intersezione dei permessi stabiliti nel parametro `mode`, da cui sono stati sottratti i permessi impostati con `umask`. Se esiste una ACL di default per la directory superiore, i bit dei permessi si compongono in base all'intersezione del valore del parametro `mode` e dei permessi stabiliti nella ACL di default e quindi assegnati all'oggetto. `umask` in questo caso non viene considerato.

ACL di default nella prassi

I tre esempi che seguono mostrano le principali operazioni per le directory e le ACL di default:

1. Aggiungere una ACL di default a una directory esistente `mydir` con:

   ```
   setfacl -d -m group:mascots:r-x mydir
   ```

   L'opzione `-d` del comando `setfacl` istruisce `setfacl` ad applicare le modifiche seguenti (opzione `-m`) alla ACL di default.

   Osservate con attenzione il risultato del comando:

   ```
   getfacl mydir

   # file: mydir
   # owner: tux
   # group: project3
   user::rwx
   user:geeko:rwx
   group::r-x
   group:mascots:rwx
   ```

```
mask::rwx
other::---
default:user::rwx
default:group::r-x
default:group:mascots:r-x
default:mask::r-x
default:other::---
```

`getfacl` ritorna sia l'ACL di accesso che quella di default. Le righe che iniziano con `default` rappresentano l'ACL di default. Anche se per quanto riguarda l'ACL di default avete passato al comando `setfacl` solamente la registrazione per il gruppo `mascots`, `setfacl` ha copiato automaticamente tutte le altre registrazioni della ACL di accesso per creare una ACL di default valida. Le ACL di default non influiscono direttamente sui permessi di accesso, hanno effetto solo quando si crea un nuovo oggetto di file system, ovvero file o directory. Per quando riguarda la trasmissione dei permessi viene presa in considerazione solo l'ACL di default della directory superiore.

2. Nel prossimo esempio create con `mkdir` una sottodirectory in `mydir` che "erediterà" l'ACL di default.

```
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::---
```

Come previsto, la nuova sottodirectory `mysubdir` ha gli stessi permessi della ACL di default della directory superiore. L'ACL di accesso di `mysubdir` è una copia perfetta della ACL di default di `mydir`, come è an-

che il caso per l'ACL di default che questa directory trasmetterà a sua volta ai propri sotto-oggetti.

3. Con `touch`, create un file nella directory `mydir`: per esempio, `touch mydir/myfile`. `ls -l mydir/myfile` adesso mostra:

   ```
   -rw-r-----+ ... tux project3 ... mydir/myfile
   ```

   L'output di `getfacl mydir/myfile` è:

   ```
   # file: mydir/myfile
   # owner: tux
   # group: project3
   user::rw-
   group::r-x          # effective:r--
   group:mascots:r-x   # effective:r--
   mask::r--
   other::---
   ```

   Da considerare in questo esempio: con `touch` si ha un `mode` con il valore `0666`, cioè i nuovi file vengono creati con permesso di accesso in lettura e scrittura per tutte e tre le categorie di utenti, a meno che `umask` o l'ACL di default non preveda altre restrizioni (si veda la sezione Gli effetti di una ACL di default a pagina 643).

   Concretamente questo significa che tutti i permessi di accesso non contenuti nel valore `mode` vengono eliminati dalle rispettive registrazioni ACL. Dalla registrazione ACL per *group class* non sono stati eliminati dei permessi, tuttavia è stata adattata la voce *mask* in modo che vengano mascherati i bit dei permessi non impostati tramite `mode`.

   In questo modo si assicura che per esempio un compiler possa interagire senza difficoltà con le ACL. Potete creare dei file con permessi di accesso limitati e contrassegnarli in seguito come eseguibili. `mask` fa sì che gli utenti e i gruppi ottengano anche i permessi concessi loro nella ACL di default.

35.3.4 L'algoritmo di controllo delle ACL

Prima che un pocesso possa accedere a un oggetto di un filesystem protetto da una ACL, viene applicato un algoritmo di controllo. In linea di principio le registrazioni ACL vengono analizzate in questa sequenza: *owner*, *named user*, *owning group* o *named group* ed *other*. E tramite la voce che più si adatta si regola quindi l'accesso. I permessi non si cumulativi.

Le cose si complicano un po' quando un processo appartiene a più di un gruppo, dunque quando teoricamente anche più registrazioni *group* potrebbero essere quelle adatte. Tra le registrazioni adatte con i permessi richiesti ne viene selezionata una a caso. Infatti per il risultato finale "Accesso consentito" non fa differenza quale voce sia stata effettivamente scelta. Se nessuna voce *group* adatta dispone dei permessi corretti, è di nuovo una voce a caso che procura il risultato finale che in questo caso sarà "access denied".

35.4 Supporto delle ACL nelle applicazioni

Come descritto nei paragrafi precedenti le ACL consentono di realizzare scenari per la concessione dei permessi di accesso davvero complessi, all'altezza anche delle applicazioni più recenti. Il modello dei permessi tradizionale e le ACL si possono coniugare in maniera eccellente. I comandi principali che riguardano i file come (`cp`, `mv`, `ls`, ...) supportano le ACL.

Purtroppo però tanti editor e file manager come (p.es. Konqueror) non supportano le ACL. Attualmente se copiate dei file con Konqueror le ACL vanno perse. Se modificate con un editor un file con ACL di accesso, dipende dal modo di back-up dell'editor utilizzato se l'ACL di accesso viene mantenuta anche a conclusione della elaborazione: Se l'editor scrive le modifiche nel file originale, l'ACL di accesso viene mantenuta. Se l'editor crea un nuovo file che dopo essere stato modificato riceve il nome del vecchio file, le ACL molto probabilmente andranno perse, a meno che l'editor non supporti le ACL. Fatta eccezione per star archiver non esistono inoltre programmi di back-up che mantengono le ACL.

35.5 Ulteriori informazioni

Informazioni dettagliate sulle ACL si trovano su `http://acl.bestbits.at/`. Si vedano anche le pagine di manuale di `getfacl(1)`, `acl(5)` e `setfacl(1)`.

Le utility per il controllo del sistema

Nel presente capitolo presenteremo una serie di programmi e meccanismi per una verifica dello stato del vostro sistema. Inoltre descriveremo delle utility di sicuro interesse per il lavoro quotidiano al sistema e relative opzioni di maggior importanza.

Per i comandi trattati vengono riportati rispettivamente degli output di carattere esemplare con il primo rigo che riporta il comando stesso (dopo un $ quale prompt), le omissioni vengono indicate con `[...]` e righi (troppo) lunghi presentano un ritorno a capo caratterizzato da un (\):

```
$ 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
```

Per poter trattare un numero quanto elevato possibile di utility ci limitiamo nella nostra illustrazione. Per il reperimento di ulteriori informazioni rimandiamo alle pagine di manuale. La maggior parte dei comandi supportano anche l'opzione `--help` che ritorna un breve elenco di tutte le opzioni consentite.

36.1 Elenco dei file aperti: lsof

Per visualizzare un elenco completo dei file aperti dal processo con l'ID di processo ⟨*PID*⟩, vi è l'opzione `-p`. Per fare un esempio: per visualizzare tutti i file utilizzati dalla shell in esecuzione si lancia:

```
$ 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
```

È stata utilizzata la variabile di shell speciale `$$` che ha come valore l'ID del processo della shell.

Senza alcuna opzione `lsof` elenca tutti i file utilizzati al momento, che di solito sarà un numero davvero considerevole. Vi sono inoltre dei modi per eseguire delle ricerche che ritornano delle liste con delle indicazioni interesse sotto un determinato punto di vista. Ad esempio si potrà voler elencare tutti i dispositivi a carattere utilizzati:

```
$ 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 Chi sta accedendo ai file: fuser

A volte può rilevarsi utile poter determinare quale processo o quale utente sta accedendo ad un file in particolare. Presupponiamo ad esempio che su `/mnt` sia montato un file system e che volete eseguire l'`umount`. Il tentativo di eseguire l'unmount fallisce: "device is busy". Con `fuser` possiamo vedere i processi che accedono al dispositivo:

```
$ fuser -v /mnt/*

                     USER        PID ACCESS COMMAND
/mnt/notes.txt
                     jj        26597 f....  less
```

Dopo aver terminato il processo `less`, in esecuzione su di un altro terminale, si può procedere con l'unmount del file system.

36.3 Caratteristiche di un file: stat

Per avere una rassegna delle caratteristiche di un file vi è il comando `stat`:

```
$ 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
```

Tramite l'opzione `--filesystem` vengono visualizzate le caratteristiche del file system nel quale si trova il file in questione:

```
 $ stat  . --filesystem
  File: "."
    ID: 0        Namelen: 255     Type: ext2/ext3
Blocks: Total: 19347388   Free: 17831731   Available: 16848938   Size: 4096
Inodes: Total: 9830400    Free: 9663967
```

Se utilizzate la z-shell (`zsh`) dovete immettere `/usr/bin/stat` dato che la z-shell ha uno shell built-in `stat` con opzioni e formato di output differenti:

```
% 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 Dispositivi USB: lsusb

Con il comando `lsusb` elencate tutti i dispositivi USB. L'opzione `-v` emette un elenco con più dettagli letti dalla directory `/proc/bus/usb/`. Segue l'output di

`lsusb` dopo aver connesso una chiave USB. L'ultimo rigo indica la presenza di un nuovo 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 Informazioni su un dispositivo SCSI: scsiinfo

Il comando `scsiinfo` fornisce delle informazioni su di un dispositivo SCSI. L'opzione `-l` elenca tutti i dispositivi SCSI rilevati dal sistema (dato simile a quello ottenuto tramite il comando `lsscsi`). Segue l' output di `scsi -i /dev/sda` che fornisce delle informazioni sul disco rigido. Con l'opzione `-a` si ottiene un numero ancora maggiore di informazioni.

```
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
```

Ci sono due elenchi di cosiddette bad page, detti anche blocchi difettosi, di un hard disk: uno messo a disposizione dal fornitore (manufacture table) e il seconda si forma con il sistema in esecuzione (la cosiddetta grown table). Se il numero delle registrazioni della grown table aumenta in modo costante, allora si consiglia di sostituire il disco rigido.

36.6 I processi: top

`top` (che sta per: table of processes) mostra un elenco dei processi che viene aggiornato ogni due secondi. Il programma viene terminato tramite il tasto ⓠ. Con l'opzione `-n 1` il programma si chiude dopo aver visualizzato una volta l'elenco dei processi. Nel seguente esempio riportiamo l'output del comando `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
```

Durante l'esecuzione di `top` premendo sul tasto ⓕ si apre un menu che vi permette di intervenire in modo molto dettagliato sul formato dell'output.

Per monitorare solo i processi di un determinato utente si utilizza l' opzione `-U UID`, laddove l' ⟨*UID*⟩ é la user-ID dell'utente. `top -U $(id -u nomeutente)` individua l'UID dell'utente in base al nome utente e visualizza i relativi processi:

36.7 Elenco dei processi: ps

Il comando `ps` ritorna un elenco dei processi. Con l'opzione `r` vengono indicati solo i processi realmente in esecuzione:

```
$ 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
```

L'opzione va aggiunta effettivamente *senza* il trattino (il segno meno). Tra le numerose opzioni ve ne sono alcune che vanno inserite senza ed altre che vanno inserite con il trattino. La pagina di manuale si addice bene a scoraggiare potenziali utenti. Per fortuna potete farvi indicare una breve pagina di assistenza con `ps --help`.

Verifichiamo quanti processi `emacs` sono in esecuzione:

```
$ 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
```

Con l'opzione `-p` i processi vengono selezionati in base all'ID del processo:

```
$ 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
```

L'elenco dei processi si lascia anche formattare in base alle proprie esigenze. Tramite l'opzione `-L` viene emesso un elenco di tutte le parole chiavi. Se volete avere un elenco dei processi disposti in base al volume di memoria occupata, utilizzate il seguente 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 Albero dei processi: pstree

Il comando `pstree` emette un elenco dei processi in una struttura ad albero:

```
$ 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
```

L'opzione `-p` aggiunge ai nomi l'ID del processo. Con l'opzione `-a` si visualizza anche la linea di comando:

```
$ 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 Chi fa cosa: w

Il comando `w` vi permette di vedere chi è loggato e le operazioni che sta eseguendo. Esempio:

```
$ 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
```

L'ultimo rigo indica che l'utente jj ha si è connesso all'host `totan` tramite una connessione secure shell (`ssh`). Se ci sono degli utenti di altri sistemi che hanno eseguito il login da remoto, l'opzione `-f` indica da quale host hanno creato la connessione.

36.10 Il carico della memoria: free

Il comando `free` indica la quantità di RAM (e swap) utilizzata ed libera:

```
$ free
             total       used       free     shared    buffers     cached
Mem:        514736     273964     240772          0      35920      42328
-/+ buffers/cache:     195716     319020
Swap:      1794736     104096    1690640
```

Utile è anche l'opzione `-m` che visualizza tutte le indicazioni di misura in megabyte:

```
$ free -m
             total       used       free     shared    buffers     cached
Mem:           502        267        235          0         35         41
-/+ buffers/cache:        191        311
Swap:         1752        101       1651
```

L'informazione davvero interessante si ha nel seguente rigo:

```
-/+ buffers/cache:        191        311
```

che calcola l'utilizzo di memoria da parte del buffer e della cache. Con l'opzione `-d delay` l'output viene aggiornato ogni ⟨*delay*⟩ di secondi: `free -d 1.5` quindi emette i valori aggiornati ogni 1,5 secondi.

36.11 Ring buffer del kernel: dmesg

Il kernel Linux memorizza una certa quantità dei suoi messaggi nel cosiddetto ring buffer. Il comando `dmesg` emette questi messaggi:

```
$ 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
```

Il penultimo rigo indica un problema di natura temporanea del server NFS `totan`. I righi antecedenti si riferiscono alla connessione di una chiave di memoria USB. Gli eventi più addietro nel tempo vengono protocollati nei file `/var/log/messages` e `/var/log/warn`.

36.12 File system: mount, df e du

Il comando `mount` mostra i punti di montaggio (ingl. mount point) dei file system (dispositivo e tipo):

```
$ 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)
```

`df` indica i file system utilizzati. L'opzione `-h` (che sta per `--human-readable`) rende l'output di comoda consultazione per l'utente:

```
$ 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
```

Chi utilizza il server di file NFS `totan` dovrebbe ripulire la propria directory home. La dimensione complessiva di tutti i file residenti in una directory si lascia determinare tramite il comando `du`. L'opzione `-s` sopprime l'emissione di un output dettagliato, con `-h` si ha un output di comoda lettura. Tramite:

```
$ du -sh ~
361M    /suse/jj
```

si vede quanto spazio occupa la propria directory home.

36.13 Il file system /proc

Nel caso del file system `/proc` ci troviamo di fronte ad uno pseudo-file system utilizzato dal kernel per archiviarvi delle informazioni importanti sotto forma di file virtuali. Ad esempio, il tipo di CPU si lascia determinare in maniera semplice nel modo seguente:

```
$ 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
[...]
```

Allocazione e utilizzo degli interrupt viene rilevato tramite:

```
$ 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
```

Segue una rassegna di file recanti informazioni importanti:

`/proc/devices` dispositivi disponibili

`/proc/modules` moduli del kernel caricati

`/proc/cmdline` linea di comando del kernel

`/proc/meminfo` informazioni dettagliate sull'utilizzo della memoria

`/proc/config.gz` file di configurazione compresso `gzip` del kernel attualmente in esecuzione

Ulteriori informazioni sono contenute nel file di testo: `/usr/src/linux/Documentation/filesystems/proc.txt`; informazioni sui processi in esecuzione si trovano nelle directory `/proc/`⟨*NNN*⟩, laddove ⟨*NNN*⟩ indica l'ID del relativo processo (PID). Sotto `/proc/self/` il processo trova le proprie caratteristiche:

```
$ 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
```

Nel file `maps` si trovano gli indirizzi degli eseguibili e delle librerie:

```
$ 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 e mpstat

L'utility `vmstat` fornisce delle statistiche riguardanti la memoria virtuale, legge i file `/proc/meminfo`, `/proc/stat` e `/proc/*/stat` ed è utile quando si vuole identificare colli di bottiglia riguardanti le prestazioni del sistema.

Il comando `iostat` fornisce delle statistiche sulla CPU nonché l'input/output dei dispositivi e partizioni. Le informazioni visualizzate provvengono dai file `/proc/stat` e `/proc/partitions`. In base all'output si potrà meglio bilanciare il carico di input ed output tra i vari dischi rigidi. Il comando `mpstat` emette delle statistiche che hanno come oggetto la CPU.

36.15 procinfo

Il programma `procinfo` riassume le informazioni principali del file system `/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
```

Per visualizzare "tutte" le informazioni vi è l'opzione `-a`. Con l'opzione `-nN` i dati vengono richiesti ogni $\langle N \rangle$ secondi. Per terminare il programma si utilizza il tasto ⓠ.

Di default vengono indicati i valori cumulativi, con l'opzione `-d` si hanno quelli differenziali: `procinfo -dn5` indica i valori che hanno subito una modifica negli ultimi 5 secondi:

```
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 Risorse PCI: lspci

Con il comando `lspci` elencate le risorse 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)
```

L'opzione `-v` ne aumenta la verbosità:

```
$ 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 risoluzione dei nomi dei dispositivi avviene tramite il file `/usr/share/pci.ids`. Le ID delle PCI non elencate in questo file vengono indicate con "Unknown device".

Con l'opzione `-vv` si ottengono tutte le informazioni possibili ed immaginabili sul programma. Per avere solo i valori numerici vi è l'opzione `-n`.

36.17 Tenere traccia delle chiamate di sistema: strace

Grazie a `strace` si può tenere traccia delle chiamate di sistema di un processo in esecuzione. Basta anteporre `strace` al comando che si intende eseguire:

```
$ 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, "strace-ls.txt  myfile.txt  strac"..., 41) = 41
munmap(0x40018000, 4096)                = 0
exit_group(0)                           = ?
```

Per seguire ad esempio tutti i tentativi di aprire un file, immettete:

```
$ 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
```

Per rintracciare tutti i processi figlio ci si serve dell'opzione `-f`. Chiaramente si può intervenire sul comportamento ed il formato di output di strace, a riguardo si consiglia di consultare `man strace`.

36.18 Le chiamate alle libreria all'esecuzione di un programma: ltrace

Le chiamate alle librerie di un processo possono essere visualizzate ricorrendo al comando `ltrace`. L'utilizzo è analogo a quello di `strace`. L'opzione `-c` emette il numero e la durata delle chiamate alle librerie eseguite:

```
$ ltrace -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 Librerie richieste: ldd

Tramite `ldd` si scopre quali librerie caricherebbe l'eseguibile dinamico indicato sotto forma di argomento:

```
$ 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)
```

Binari statici chiaramente non richiedono librerie dinamiche:

```
$ 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 Ulteriori informazioni sui file binari ELF

Il programma `readelf` legge il contenuto di file binari. Ciò funziona anche con file ELF assemblati per una architettura diversa:

```
$ 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 Comunicazione tra i processi: ipcs

Il comando `ipcs` ritorna un elenco delle risorse IPC utilizzate:

```
$ 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 Misurare il tempo con time

Il tempo richiesto dai comandi si lascia determinare tramite l'utility `time`. Questo programma è disponibile in due versioni: come shell-builtin e come programma (sotto `/usr/bin/time`).

```
$ time find . > /dev/null

real    0m4.051s
user    0m0.042s
sys     0m0.205s
```

Parte V

Appendice

Fonti di informazione e documentazione

Questo capitolo vi indica dove reperire ulteriori informazioni ed ulteriore documentazione riguardanti il vostro sistema SUSE LINUX. Alcune fonti sono proprie di SUSE, ma la maggior parte dei casi si tratta di fonte di più ampio respiro. Alcune saranno disponibili a sistema installato o mezzo di installazione, altre saranno accessibili tramite Internet.

Documentazione SUSE

Sono a vostra disposizione i nostri manuali in formato HTML o PDF che trovate nei pacchetti RPM `suselinux-adminguide_it` e `suselinux-adminguide_it`). Nel corso di una installazione standard i manuali vengono archiviati nella directory `/usr/share/doc/manual/`. Tramite il SUSEHelpCenter potrete accedere a queste fonti.

Il Linux Documentation Projekt (TLDP)

Il Linux Documentation Projekt (si veda `http://www.tldp.org/`) è un gruppo di volontari che si occupa della stesura della documentazione incentrata su Linux. TLDP offre degli HOWTO, FAQ, guide e pubblicato sotto una licenza libera.

Gli HOWTO illustrano i singoli passi da seguire per raggiungere un determinato obiettivo e si rivolgono a utenti finali, amministratori di sistema oppure programmatori. In un HOWTO ad esempio viene trattato il modo di configurare un server DHCP e indicato cosa vi è da tenere presente, non però come installare Linux

come tale. In linea di massima gli HOWTO contengono delle indicazioni generali in modo da poter essere applicate a ogni distribuzione. Il pacchetto `howto` contiene degli HOWTO in ASCII. Gli utenti che preferiscono HTML, installino `howtoenh`.

Le FAQ (ingl. Frequently Asked Questions) sono delle raccolte di domande e risposte su tematiche che vengono trattate spesso nelle mailing list. Le domande sono del tipo: "Cos'è LDAP?", "Cos'è RAID?" etc. Le FAQ sono in genere dei testi piuttosto brevi.

Le cosiddette Guide sono dei manuali che trattano un determinato tema in modo più dettagliato rispetto agli HOWTO o alle FAQ. Vi sono ad esempio delle guide incentrate sulla programmazione del kernel, amministrazione della rete, etc. L'obiettivo è quello di dare al lettore il modo di approfondire le sue conoscenza in un determinato campo.

Alcune fonti di documentazione del TLDP sono disponibili anche in altri formati, ad esempio nel formato PDF, sotto forma di pagine HTML singole e multiple, nel formato PostScript e come sorgenti SGML/XML. A volte vi sono anche dei documenti che sono stati tradotti in varie lingue.

Pagine man e info

Una pagina di manuale (ingl. manual page) è un testo di aiuto riferito ad un comando, chiamata di sistema, formato file e simili. Di solito una pagina di manuale è suddivisa in diverse sezioni come nome, sintassi, descrizione, opzioni, file, etc.

Per avere una pagina di manuale immettete: `man ls`. Questa immissione mostra il testo di aiuto per il comando `ls`. Con i tasti cursore potete scorrere il testo, con ⓠ uscite da `man`. Per stampare una pagine di manuale (ad esempio per il comando `ls`), immettete: `man -Tps | lpr` Per avere ulteriori informazioni sul comando (`man man`).

Della documentazione è disponibile anche nel formato info, ad esempio su `grep`. Il comando è:

```
info grep
```

A differenza delle pagine di manuale, le pagine info sono più articolate e composte da diversi cosiddetti "nodi". Un nodo visualizza una pagina da poter scorrere con un Info Reader (comparabile ad un browser HTML). Per navigare all'interno di una pagina info si ricorre ai tasti ⓟ (previous, per pagina precedente) e

ⓝ (next, per la pagina successiva). Con ⓠ uscite da `info`. Le funzioni di ulteriori tasti è reperibile nella documentazione dedicata a `info` (invocate `info info`).

Sia le pagine di manuale che pagine info possono essere lanciate dalla riga Url di Konqueror immettendo `man:`⟨*comando*⟩ o `info:`⟨*comando*⟩.

Standard e specificazioni

Se cercate delle informazioni riguardanti degli standard o delle specificazioni potete attingere a diverse fonti:

`www.linuxbase.org` Il Free Standards Group è una organizzazione indipendente non-profit, il cui obiettivo è quello di promuovere la divulgazione del software a sorgente aperto e libero tramite la definizione di standard validi per tutte le distribuzioni. Sotto la guida di questa organizzazione vengono mantenuti diversi standard, tra cui LSB (Linux Standard Base) uno dei più importanti nel mondo di Linux.

`http://www.w3.org` Il World Wide Web Consortium (W3C) è sicuramente una delle più note istituzioni, istituita nell'ottobre del 1994 da TimBerners-Lee focalizzata sulla standardizzazione di tecnologie web. Sostiene la diffusione di specificazioni non vincolate ad un produttore e non sottoposte a licenza, ad esempio HTML, XHTML, XML e altri. Questi "web standard" vengono formalizzati nel corso di un processo composto da 4 fasi da cosiddetti *working groups* e presentati al pubblico sotto forma di *W3C Recommendation* (REC).

`http://www.oasis-open.org` OASIS (Organization for the Advancement of Structured Information Standards) è un consorzio internazionale specializzato nello sviluppo di standard in ambito web security, e-Business, scambi commerciali, logistica e l'interoperabilità tra mercati diversi.

`http://www.ietf.org` L' Internet Engineering Task Force (IETF) è una comunità di ricercatori, network designer, fornitori ed utenti operante a livello internazionale che si dedica allo sviluppo dell'architettura Internet e del funzionamento senza intoppi dell'Internet tramite dei protocolli.

Ogni standard IETF viene pubblicato sotto forma di RFC (Request for Comments ed è gratuito. Vi sono sei tipi di RFC: propsed standards, draft standards, Internet standards, experimental protocols, Informational documents

e historic standards. Solo i primi tre (proposed, draft, e full) sono degli standard IETF nel senso più stretto (si veda a riguardo anche il riassunto da poter consultare sotto `http://www.ietf.org/rfc/rfc1796.txt`).

`http://www.ieee.org` L' Institute of Electrical and Electronics Engineers (IEEE) si occupa della definizione di standard in ambito della tecnologia dell'informazione, telecomunicazione, medico- sanitario, dei trasporti e altro. Gli standard IEEE non sono gratuiti.

`http://www.iso.org` Il comitato ISO (International Organization for Standards) è uno dei maggiori attori sul campo della definizione di standard e si appoggia su una rete di istituti di standardizzazione nazionali in oltre 140 paesi. Gli standard ISO non sono gratuiti.

Verifica del file system

Pagina di man di 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 parti
   tion  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)
```

Pagina di man di 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 multiple 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).

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)
```

Traduzione italiana della GNU General Public License

Questa è una traduzione italiana non ufficiale della Licenza Pubblica Generale GNU. Non è pubblicata dalla Free Software Foundation e non ha valore legale nell'esprimere i termini di distribuzione del software che sottostà alla licenza GPL. Ad ogni modo, speriamo che questa traduzione aiuti le persone di lingua italiana a capire meglio il significato della licenza GPL

La *Free Software Foundation* (FSF) non è l'editore di questa traduzione e non la riconosce come surrogato con valore di legge per l'originale-GNU-GPL (si veda `http://www.gnu.org/copyleft/gpl.html`). Dato che la traduzione non è stata verificata in modo approfondito da legali non può essere garantito che la traduzione rispecchia in modo esatto quando dichiarato nella GNU-GPL. Per essere sicuri che l'utilizzo progettato sia consentito attenetevi alla versione originale in inglese.

La *Free Software Foundation* vi prega di non utilizzare questa traduzione come fonte ufficiale per software da voi scritto; fate invece direttamente riferimento alla versione originale in inglese pubblicata della *Free Software Foundation*.

This is a translation of the GNU General Public License into Italian. 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.

LICENZA PUBBLICA GENERICA (GPL) DEL PROGETTO GNU

Traduzione italiana, versione 2, Giugno 1991

59 Temple Place, Suite 330, Boston, MA 02111-1307, USA

Traduzione curata dal gruppo Pluto e da ILS, ultimo aggiornamento, 30 luglio 1998.

Importante

Questa traduzione non è un surrogato con validità legale per la versione originale in inglese!

Importante

Preambolo

Le licenze per la maggioranza dei programmi hanno lo scopo di togliere all'utente la libertà di condividerlo e di modificarlo. Al contrario, la Licenza Pubblica Generica GNU è intesa a garantire la libertà di condividere e modificare il free software, al fine di assicurare che i programmi siano "liberi" per tutti i loro utenti. Questa Licenza si applica alla maggioranza dei programmi della *Free Software Foundation* e ad ogni altro programma i cui autori hanno scelto questa Licenza. Alcuni altri programmi della *Free Software Foundation* sono invece coperti dalla Licenza Pubblica Generica per Librerie. Chiunque può usare questa Licenza per i propri programmi.

Quando si parla di *software "free"*, ci si riferisce alla libertà, non al prezzo. Le nostre Licenze (la GPL e la LGPL) sono progettate per assicurarsi che c iascuno abbia la libertà di distribuire copie del free software (e farsi pagare per questo, se vuole), che ciascuno riceva il codice sorgente o che lo possa ottenere se lo desidera, che ciascuno possa modificare il programma o usarne delle parti in nuovi programmi " liberi" e che ciascuno sappia di potere fare queste cose.

Per proteggere i diritti dell'utente, abbiamo bisogno di creare delle restrizioni che vietino a chiunque di negare questi diritti o di chiedere di rinunciarvi. Queste

restrizioni si traducono in certe responsabilità per chi distribuisce copie del software e per chi lo modifica.

Per esempio, chi distribuisce copie di un Programma coperto da GPL, sia gratis sia in cambio di un compenso, deve dare ai destinatari tutti i diritti che ha ricevuto. Deve anche assicurarsi che i destinatari ricevano o possano ricevere il codice sorgente. E deve mostrar loro queste condizioni di Licenza, in modo che conoscano i loro diritti.

Proteggiamo i diritti dell'utente in due modi: (1) proteggendo il software con un copyright, e (2) offrendo una Licenza che offre il permesso legale di copiare, distribuire e/o modificare il Programma.

Infine, per proteggere ogni autore e noi stessi, vogliamo assicurarci che ognuno capisca che non ci sono garanzie per i programmi coperti da GPL. Se il Programma viene modificato da qualcun altro e ridistribuito, vogliamo che gli acquirenti sappiano che ciò che hanno non è l'originale, in modo che ogni problema introdotto da altri non si rifletta sulla reputazione degli autori originari.

Infine, ogni programma libero è costantemente minacciato dai brevetti sui programmi. Vogliamo evitare il pericolo che chi ridistribuisce un Programma libero ottenga brevetti personali, rendendo perciò il Programma una cosa di sua proprietà. Per prevenire questo, abbiamo chiarito che ogni prodotto brevettato debba essere distribuito per il libero uso da parte di chiunque, o non distribuito affatto.

Seguono i termini e le condizioni precisi per la copia, la distribuzione e la modifica.

LICENZA PUBBLICA GENERICA GNU

TERMINI E CONDIZIONI PER LA COPIA, LA DISTRIBUZIONE E LA MODIFICA

0. Questa Licenza si applica a ogni Programma o altra opera che contenga una nota da parte del detentore del copyright che dica che tale opera può distribuita sotto i termini di questa Licenza Pubblica Generica. Il termine "Programma" nel seguito indica ognuno di questi programmi o lavori, e l'espressione "lavoro basato sul Programma" indica sia il Programma sia ogni opera considerata derivata in base alla legge sul Copyright: cioè un lavoro contenente il programma o una porzione di esso, sia letteralmente sia modificato e/o tradotto in un'altra lingua; da qui in avanti, la traduzione è in ogni caso considerata una "modifica". Vengono ora elencati i diritti dei detentori di licenza.

Attività diverse dalla copiatura, distribuzione e modifica non sono coperte da questa Licenza e sono al di fuori della sua influenza. L'atto di eseguire il programma non viene limitato, e l'output del programma ècoperto da questa Licenza solo se il suo contenuto costituisce un lavoro basato sul Programma (indipendentemente dal fatto che sia stato creato eseguendo il Programma). In base alla natura del Programma il suo output può essere o meno coperto da questa Licenza.

1.È lecito copiare e distribuire copie letterali del codice sorgente del Programma così come viene ricevuto, con qualsiasi mezzo, a condizione che venga riprodotta chiaramente su ogni copia una appropriata nota di copyright e di assenza di garanzia; che si mantengano intatti tutti i riferimenti a questa Licenza e all'assenza di ogni garanzia; che si dia a ogni altro destinatario del Programma una copia di questa Licenza insieme al Programma.

2. È possibile richiedere un pagamento per il trasferimento fisico di una copia del Programma, è anche possibile a propria discrezione richiedere un pagamento in cambio di una copertura assicurativa.

È lecito modificare la propria copia o copie del Programma, o parte di esso, creando perciò un lavoro basato sul Programma, e copiare o distribuire queste modifiche e questi lavori sotto i termini del precedente punto 1, a patto che anche tutte queste condizioni vengano soddisfatte:

1. Bisogna indicare chiaramente nei file che si tratta di copie modificate e la data di ogni modifica.
2. Bisogna fare in modo che ogni lavoro distribuito o pubblicato, che in parte o nella sua totalità derivi dal Programma o da parti di esso, sia globalmente utilizzabile da terze parti secondo le condizioni di questa licenza.
3. Se di solito il programma modificato legge comandi interattivamente quando eseguito, bisogna fare in modo che all'inizio dell'esecuzione interattiva usuale, stampi un messaggio contenente una appropriata nota di copyright e di assenza di garanzia (oppure che specifichi il tipo di garanzia che si offre). Il messaggio deve inoltre specificare agli utenti che possono ridistribuire il programma nelle condizioni qui descritte e deve indicare come reperire questa licenza. Se però il programma di partenza è interattivo ma normalmente non stampa tale messaggio, non occorre che un lavoro derivato lo stampi.

Questi requisiti si applicano al lavoro modificato nel suo complesso. Se sussistono parti identificabili del lavoro modificato che non siano derivate dal Programma e che possono essere ragionevolmente considerate lavori indipendenti,

allora questa Licenza e i suoi termini non si applicano a queste parti quando vengono distribuite separatamente. Se però queste parti vengono distribuite all'interno di un prodotto che è un lavoro basato sul Programma, la distribuzione di questo prodotto nel suo complesso deve avvenire nei termini di questa Licenza, le cui norme nei confronti di altri utenti si estendono a tutto il prodotto, e quindi ad ogni sua parte, chiunque ne sia l'autore.

Sia chiaro che non è nelle intenzioni di questa sezione accampare diritti su lavori scritti interamente da altri, l'intento è piuttosto quello di esercitare il diritto di controllare la distribuzione di lavori derivati o dal Programma o contenenti esso.

Inoltre, se il Programma o un lavoro derivato da esso viene aggregato ad un altro lavoro non derivato dal Programma su di un mezzo di immagazzinamento o di distribuzione, il lavoro non derivato non deve essere coperto da questa licenza.

3. È lecito copiare e distribuire il Programma (o un lavoro basato su di esso, come espresso al punto 2) sotto forma di codice oggetto o eseguibile sotto i termini dei precedenti punti 1 e 2, a patto che si applichi una delle seguenti condizioni:

1. Il Programma sia corredato dal codice sorgente completo, in una forma leggibile dal calcolatore e tale sorgente deve essere fornito secondo le regole dei precedenti punti 1 e 2 su di un mezzo comunemente usato per lo scambio di programmi. Oppure:

2. Il Programma sia accompagnato da un'offerta scritta, valida per almeno tre anni, di fornire a chiunque ne faccia richiesta una copia completa del codice sorgente, in una forma leggibile dal calcolatore, in cambio di un compenso non superiore al costo del trasferimento fisico di tale copia, che deve essere fornita secondo le regole dei precedenti punti 1 e 2 su di un mezzo comunemente usato per lo scambio di programmi. Oppure:

3. Il Programma sia accompagnato dalle informazioni che sono state ricevute riguardo alla possibilità di avere il codice sorgente. Questa alternativa è permessa solo in caso di distribuzioni non commerciali e solo se il programma è stato ricevuto sotto forma di codice oggetto o eseguibile in accordo al precedente punto.

Per codice sorgente completo di un lavoro si intende la forma preferenziale usata per modificare un lavoro. Per un programma eseguibile,"codice sorgente completo" significa tutto il codice sorgente di tutti i moduli in esso contenuti, più ogni file associato che definisca le interfacce esterne del programma, più gli script usati per controllare la compilazione e l' installazione dell'eseguibile. In ogni caso

non è necessario che il codice sorgente fornito includa nulla che sia normalmente distribuito (in forma sorgente o in formato binario) con i principali componenti del sistema operativo sotto cui viene eseguito il Programma (compilatore, kernel, e così via), a meno che tali componenti accompagnino l'eseguibile.

Se la distribuzione dell'eseguibile o del codice oggetto è effettuata indicando un luogo dal quale sia possibile copiarlo, permettere la copia del codice sorgente dallo stesso luogo è considerata una valida forma di distribuzione del codice sorgente, anche se copiare il sorgente è facoltativo per l'acquirente.

4.Non è lecito copiare, modificare, sublicenziare, o distribuire il Programma in modi diversi da quelli espressamente previsti da questa Licenza. Ogni tentativo di copiare, modificare, sublicenziare o distribuire il Programma non è autorizzato, e farà terminare automaticamente i diritti garantiti da questa Licenza. D'altra parte ogni acquirente che abbia ricevuto copie, o diritti, coperti da questa Licenza da parte di persone che violano la Licenza come qui indicato non vedranno invalidare la loro Licenza, purchè si comportino conformemente ad essa.

5. L'acquirente non è obbligato ad accettare questa Licenza, poichè non l'ha firmata. D'altra parte nessun altro documento garantisce il permesso di modificare o distribuire il Programma o i lavori derivati da esso. Queste azioni sono proibite dalla legge per chi non accetta questa Licenza; perciò, modificando o distribuendo il Programma o un lavoro basato sul programma, si indica nel fare ciò l'accettazione di questa Licenza e quindi di tutti i suoi termini e le condizioni poste sulla copia, la distribuzione e la modifica del Programma o di lavori basati su di esso.

6. Ogni volta che il Programma o un lavoro basato su di esso vengono distribuiti, l'acquirente riceve automaticamente una licenza d'uso da parte del licenziatario originale. Tale licenza regola la copia, la distribuzione e la modifica del Programma secondo questi termini e queste condizioni. Non è lecito imporre restrizioni ulteriori al- l'acquirente nel suo esercizio dei diritti qui garantiti. Chi distribuisce programmi coperti da questa Licenza non e' comunque responsabile per la conformità alla Licenza da parte di terze parti.

7. Se, come conseguenza del giudizio di una corte, o di una imputazione per la violazione di un brevetto o per ogni altra ragione (anche non relativa a questioni di brevetti), vengono imposte condizioni che contraddicono le condizioni di questa licenza, che queste condizioni siano dettate dalla corte, da accordi tra le parti o altro, queste condizioni non esimono nessuno dall'osservazione di questa Licenza. Se non è possibile distribuire un prodotto in un modo che soddisfi simultaneamente gli obblighi dettati da questa Licenza e altri obblighi pertinenti, il prodotto non può essere affatto distribuito. Per esempio, se un brevetto non permettesse

a tutti quelli che lo ricevono di ridistribuire il Programma senza obbligare al pagamento di diritti, allora l'unico modo per soddisfare contemporaneamente il brevetto e questa Licenza e' di non distribuire affatto il Programma.

Se parti di questo punto sono ritenute non valide o inapplicabili per qualsiasi circostanza, deve comunque essere applicata l'idea espressa da questo punto; in ogni altra circostanza invece deve essere applicato il punto 7 nel suo complesso.

Non è nello scopo di questo punto indurre gli utenti ad infrangere alcun brevetto nè ogni altra rivendicazione di diritti di proprietà, nè di contestare la validità di alcuna di queste rivendicazioni; lo scopo di questo punto è solo quello di proteggere l'integrità del sistema di distribuzione dei programmi liberi, che viene realizzato tramite l'uso della licenza pubblica. Molte persone hanno contribuito generosamente alla vasta gamma di programmi distribuiti attraverso questo sistema, basandosi sull'applicazione fedele di tale sistema. L'autore/donatore può decidere di sua volontà se preferisce distribuire il software avvalendosi di altri sistemi, e l'acquirente non può imporre la scelta del sistema di distribuzione.

Questo punto serve a rendere il più chiaro possibile ciò che crediamo sia una conseguenza del resto di questa Licenza.

8.Se in alcuni paesi la distribuzione e/o l'uso del Programma sono limitati da brevetto o dall'uso di interfacce coperte da copyright, il detentore del copyright originale che pone il Programma sotto questa Licenza può aggiungere limiti geografici espliciti alla distribuzione, per escludere questi paesi dalla distribuzione stessa, in modo che il programma possa essere distribuito solo nei paesi non esclusi da questa regola. In questo caso i limiti geografici sono inclusi in questa Licenza e ne fanno parte a tutti gli effetti.

9.All'occorrenza la *Free Software Foundation* può pubblicare revisioni o nuove versioni di questa Licenza Pubblica Generica. Tali nuove versioni saranno simili a questa nello spirito, ma potranno differire nei dettagli al fine di coprire nuovi problemi e nuove situazioni.

Ad ogni versione viene dato un numero identificativo. Se il Programma asserisce di essere coperto da una particolare versione di questa Licenza e "da ogni versione successiva" *("any later version")*, l' acquirente può scegliere se seguire le condizioni della versione specificata o di una successiva. Se il Programma non specifica quale versione di questa Licenza deve applicarsi, l'acquirente può scegliere una qualsiasi versione tra quelle pubblicate dalla *Free Software Foundation*.

10. Se si desidera incorporare parti del Programma in altri programmi liberi le cui condizioni di distribuzione differiscano da queste, è possibile scrivere all' autore del Programma per chiederne l'autorizzazione. Per il software il cui copyright

è detenuto dalla *Free Software Foundation*, si scriva alla *Free Software Foundation*; talvolta facciamo eccezioni alle regole di questa Licenza. La nostra decisione sarà guidata da due scopi: preservare la libertà di tutti i prodotti derivati dal nostro free software e promuovere la condivisione e il riutilizzo del software in generale.

>NON C'È GARANZIA

11. POICHÈ IL PROGRAMMA È CONCESSO IN USO GRATUITAMENTE, NON C'È GARANZIA PER IL PROGRAMMA, NEI LIMITI PERMESSI DALLE VIGENTI LEGGI. SE NON INDICATO DIVERSAMENTE PER ISCRITTO, IL DETENTORE DEL COPYRIGHT E LE ALTRE PARTI FORNISCONO IL PROGRAMMA "COSÌ COM'È", SENZA ALCUN TIPO DI GARANZIA, NÈ ESPLICITA NÈ IMPLICITA; CIÒ COMPRENDE, SENZA LIMITARSI A QUESTO, LA GARANZIA IMPLICITA DI COMMERCIABILITÀ E UTILIZZABILITÀ PER UN PARTICOLARE SCOPO. L'INTERO RISCHIO CONCERNENTE LA QUALITÀ E LE PRESTAZIONI DEL PROGRAMMA È DELL'ACQUIRENTE. SE IL PROGRAMMA DOVESSE RIVELARSI DIFETTOSO, L'ACQUIRENTE SI ASSUME IL COSTO DI OGNI MANUTENZIONE, RIPARAZIONE O CORREZIONE NECESSARIA.

12. NÈ IL DETENTORE DEL COPYRIGHT NÈ ALTRE PARTI CHE POSSONO MODIFICARE O RIDISTRIBUIRE IL PROGRAMMA COME PERMESSO IN QUESTA LICENZA SONO RESPONSABILI PER DANNI NEI CONFRONTI DELL'ACQUIRENTE, A MENO CHE QUESTO NON SIA RICHIESTO DALLE LEGGI VIGENTI O APPAIA IN UN ACCORDO SCRITTO. SONO INCLUSI DANNI GENERICI, SPECIALI O INCIDENTALI, COME PURE I DANNI CHE CONSEGUONO DALL'USO O DALL'IMPOSSIBILITÀ DI USARE IL PROGRAMMA; CIÒ COMPRENDE, SENZA LIMITARSI A QUESTO, LA PERDITA DI DATI, LA CORRUZIONE DEI DATI, LE PERDITE SOSTENUTE DALL'ACQUIRENTE O DA TERZE PARTI E L'INABILITÀ DEL PROGRAMMA A LAVORARE INSIEME AD ALTRI PROGRAMMI, ANCHE SE IL DETENTORE O ALTRE PARTI SONO STATE AVVISATE DELLA POSSIBILITÀ DI QUESTI DANNI.

FINE DEI TERMINI E DELLE CONDIZIONI

Appendice: come applicare questi termini ai nuovi programmi

Se si sviluppa un nuovo programma e lo si vuole rendere della maggiore utilità possibile per il pubblico, la cosa migliore da fare è rendere tale programma free

software, cosicchè ciascuno possa ridistribuirlo e modificarlo sotto questi termini.

Per fare questo, si inserisca nel programma la seguente nota. La cosa migliore da fare è mettere la nota all'inizio di ogni file sorgente, per chiarire nel modo più efficiente possibile l'assenza di garanzia; ogni file dovrebbe contenere almeno la nota di copyright e l'indicazione di dove trovare l'intera nota.

```
<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.
```

In italiano:

```
<Nome del programma e una breve descrizione>

Copyright (C) <anno> <Nome dell'autore>

Questo programma è free software; è lecito redistribuirlo e/o
modificarlo secondo i termini della Licenza Pubblica Generica GNU
come è pubblicata dalla Free Software Foundation; o la versione 2
della licenza o (a propria scelta) una versione successiva.

Questo programma è distribuito nella speranza che sia utile, ma
SENZA ALCUNA GARANZIA; senza neppure la garanzia implicita di
NEGOZIABILITÀ o di APPLICABILITÀ PER UN PARTICOLARE SCOPO.
Si veda la Licenza Pubblica Generica GNU per avere maggiori dettagli.

Ognuno dovrebbe avere ricevuto una copia della Licenza Pubblica
Generica GNU insieme a questo programma; in caso contrario, si scriva
alla Free Software Foundation, Inc.,59 Temple Place, Suite 330,
Boston, MA 02111-1307, USA.
```

Si aggiungano anche informazioni su come si può essere contattati tramite posta elettronica e cartacea.

Se il programma è interattivo, si faccia in modo che stampi una breve nota simile a questa quando viene usato interattivamente:

```
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.
```

In italiano:

```
Gnomovision versione 69, Copyright (C) <anno> <nome dell'
autore>

Gnomovision non ha ALCUNA GARANZIA; per i dettagli si digiti 'show
g'.  Questo è free software, e ognuno è libero di ridistribuirlo
sotto certe condizioni; si digiti 'show c' per dettagli.
```

Gli ipotetici comandi `show w`e `show c` mostreranno le parti appropriate della Licenza Pubblica Generica. Chiaramente, i comandi usati possono essere chiamati diversamente da `show c` e `show c`; possono anche essere selezionati con il mouse o attraverso un menù; in qualunque modo pertinente al programma.

Se necessario, si dovrebbe anche far firmare al proprio datore di lavoro (se si lavora come programmatore) o alla propria scuola, se si è studente, una rinuncia al copyright per il programma. Ecco un esempio con nomi fittizi:

```
Yoyodyne, Inc., hereby disclaims all copyright interest in the
program 'Gnomovision' (which makes passes at compilers) written
by James Hacker.

signature of Ty Coon, 1st April 1989 Ty Coon, President of Vice
```

In italiano:

```
Yoyodinamica SPA rinuncia con questo documento ad ogni interesse al
copyright del programma 'Gnomovision' (che svolge dei passi di
compilazione) scritto da Giovanni Smanettone.

Firma di Primo Tizio, 1 Aprile 1999 Primo Tizio, Presidente
```

I programmi coperti da questa Licenza Pubblica Generica non possono essere incorporati all'interno di programmi proprietari. Se il proprio programma è una libreria di funzioni, può essere più utile permettere di collegare applicazioni proprietarie alla libreria. Se si ha questa intenzione consigliamo di usare la Licenza Generica Pubblica GNU per Librerie (LGPL) al posto di questa Licenza.

Glossario

Permessi di accesso
I permessi di accesso di un file determinano se un utente o gruppo possa leggere, scrivere o eseguire un file o una directory. Questi permessi vengono di solito impostati dall'amministratore.

Account
Un account è definito dallo username (o nome dell'utente o login name) e dalla password. Un account corrisponde ad una ID dell'utente (UID).

ACL (Access Control List)
Un'estensione del tradizionale concetto di permessi di accesso per file e directory che permettono di cesellare i permessi di accesso.

ADSL (Asymmetric Digital Subscriber Line)
ADSL, linea digitale asimmetrica, protocollo di trasmissione veloce che utilizza la rete telefonica.

AGP (Accelerated Graphics Port)
Bus ad alta velocità per le schede grafiche. Offre maggiore larghezza di banda. Inoltre, le schede grafiche AGP possono adoperare direttamente la RAM (senza dover passare per il processore).

ATAPI (Advanced Technology Attachment Packet Interface)
ATAPI è un tipo di lettore di CD-ROM che può essere collegato ad un controller (E)IDE. Oltre ai lettori ATAPI, esistono i lettori CD-ROM SCSI, gestiti da un controller SCSI.

Backup
Backup è il termine inglese per indicare le copie di sicurezza. È importante creare regolarmente copie di sicurezza, soprattutto dei file importanti.

Larghezza di banda
Tasso di trasferimento massimo di un canale per la trasmissione dei dati. Di solito trova impiego con connessioni di rete.

BIOS (Basic Input Output System)
Piccola componente che si occupa dell'inizializzazione di importanti processi hardware. La maggior parte dei BIOS consente di modificare parametri del sistema di basso livello per via di un programma di setup interattivo. Il codice del programma risiede in un chip read-only memory (ROM)...

Bookmark (con browser)
Segnalibro, in una raccolta di URL.

Boot
La sequenza di operazioni del computer dall'accensione fino al momento in cui il sistema è pronto per essere usato.

Browser
Il browser visualizza il contenuto di pagine locali o di pagine web.

Client
Computer all'interno di una rete che richiede delle informazioni daun server.

Linea di comando
Modo basato su testo per eseguire dei comandi.

Console
Mentre, una volta, il termine "console" era sinonimo di *terminale*, Linux vi offre delle *console virtuali*, che permettono di usare lo schermo per sessioni parallele, ma completamente indipendenti fra loro.

CPU (Central Processing Unit)
Si veda Processore.

Cursore
Il cursore è un carattere (di solito rettangolare) che indica il posto dello schermo in cui appaiono le immissioni con la tastiera.

Daemon
Un daemon disk and execution monitor è un programma che gira in sottofondo ed entra in azione in caso di necessità. Ad esempio, il demone HTTP (httpd) risponde alle richieste HTTP.

DDC (Direct Display Channel)
Standard di comunicazione tra lo schermo e la scheda grafica che permette la trasmissione di vari parametri, tra i quali il nome dello schermo o la risoluzione della scheda grafica.

Directory in un file system
Il termine "directory" (la cui poco nota traduzione italiana è "indirizzario") indica i componenti di un file system. Una directory contiene, a sua volta, file e sottodirectory.

DNS (Domain Name System)
Un sistema che converte gli indirizzi basati su nome in indirizzi IP e viceversa.

Driver
Il driver o unità (di) disco è un programma che permette la comunicazione tra il sistema operativo e l'hardware.

E-Mail (electronic mail)
Procedimento di trasmissione di `lettere elettroniche` tra utenti di una rete locale o di sistemi collegati ad Internet. Un indirizzo e-mail ha la seguente forma `username@domain.org`.

EIDE (Enhanced Integrated Drive Electronics)
Standard IDE ottimizzato che permette l'uso di dischi rigidi con dimensioni superiori a 512 MByte.

Ambiente (environment)
Le variabili di ambiente ed i rispettivi valori mantenuti da una shell. L'utente può modificare il valore di variabili date. Per un'impostazione permanente vi sono i file di configurazione della shell.

Variabile d'ambiente (environment variable)
Una elemento dell'ambiente della shell.

Ethernet
Uno degli standard per la trasmissione dati in reti di computer.

EXT2 (Second Extended File system)
Il file system usato da Linux.

FAQ (Frequently Asked Questions)
Un termine ormai entrato nell'uso corrente e che sta ad indicare tutti quei documenti che contengono le risposte alle domande più frequenti.

Firewall
Il "muro di fuoco" è un sistema che connette una rete locale ad Internet con diversi accorgimenti di sicurezza.

FTP (file transfer protocol)
Un protocollo basato su TCP/IP per la trasmissione di file via rete.

GNOME (GNU Network Object Model Environment)
Ambiente desktop grafico per Linux.

GNU (GNU is Not Unix)
GNU è un progetto della Free Software Foundation (FSF). Lo scopo del Progetto GNU è quello di creare un sistema operativo *libero* compatibile con Unix; in questo caso *libero* non vuol dire tanto *gratuito*, quanto piuttosto accessibile a tutti gli utenti. Al fine di garantire che il codice *sorgente* (cioè il codice del programma) resti tale, ogni sua modifica o aggiunta dovrà, a sua volta, essere accessibile a tutti. Come ciò sia possibile, viene spiegato dettagliatamente nel classico manifesto di GNU (`http://www.gnu.org/gnu/manifesto.html`); il software di GNU è legalmente protetto dalla licenza GNU General Public License o *GPL* (`http://www.gnu.org/copyleft/gpl.html`), nonché dalla licenza GNU Lesser General Public License (precedentemente nota come *GNU Library General Public License*) o *LGPL* (`http://www.gnu.org/copyleft/lgpl.html`) Anche il kernel Linux è protetto dalla GPL e beneficia del Progetto (soprattutto, delle nuove funzionalità), ma si dovrebbero fare le debite distinzioni.

GPL (GNU GENERAL PUBLIC LICENSE)
Vd. GNU.

Directory home
La vostra directory personale all'interno del file system di Linux. Questa directory appartiene ad un utente specifico (solitamente identificato dallo `/home/<username>`). Una directory home è pienamente accessibile solo al suo proprietario.

Hostname
Il nome di un computer tramite il quale può essere raggiunto anche sulla rete.

HTML (HyperText Markup Language)
Il linguaggio di rappresentazione di contenuti più importante del World Wide Web. I comandi di formattazione dell'HTML definiscono l'aspetto di un documento ed il modo in cui esso debba essere rappresentato da un browser.

HTTP (HyperText Transfer Protocol)
Un protocollo di rete che definisce il modo in cui richiedere e trasferire dei documenti attravcerso il World Wide Web. Di solito si tratta di documenti HTML offerti da un server e richesti da un utente tramite il browser.

IDE (Integrated Drive Electronics)
Uno standard di disco rigido estremamente diffuso nei computer del segmento medio-basso.

Internet
Rete mondiale di computer, basata sul protocollo TCP/IP.

Indirizzo IP
Un indirizzo numerico, formato da quattro blocchi separati da punti (es: 192.168.10.1) .

IRQ (Interrupt Request)
Un richiesta (asincrona) per alcune operazioni che possono essere innescate da hardware o software. Il sistema operativo gestisce la maggioranza delle IRQ

ISDN (Integrated Services Digital Network)
Diffuso standard digitale per il trasferimento di dati ad alta velocità tramite la rete telefonica.

KDE (K Desktop Environment)
Un ambiente desktop grafico per Linux.

Kernel
Il "cuore" del sistema operativo di Linux, che gestisce la memoria e file system, contiene driver per la comunicazione con dispositivi hardware e gestisce inoltre processi ed il networking

LAN (local area network)
Una LAN è una rete locale ed è solitamente piuttosto piccola.

LILO (LInux LOader)
Piccolo programma, installato nel settore di avvio del disco rigido, che può avviare non solo Linux, ma anche altri sistemi operativi.

Link
Un link ("collegamento") è un riferimento ad un file, usato sia su Internet sia nel file system di Linux. Su Linux, si distingue tra gli *hard* link (i collegamenti "rigidi") ed i link *symbolic* (simbolici) mentre gli hard link si riferiscono alla posizione esatta del documento all'interno del file system, i link *simbolici* riportano solo al nome del file.

Linux
Sistema operativo ad alte prestazioni simile a UNIX, liberamente distribuito sotto la licenza GPL (GNU). Il nome è un'abbreviazione di *Linus' uniX* e si riferisce al suo creatore, Linus Torvalds Nonostante il nome Linux si riferisca in senso stretto al solo kernel, esso viene comunemente usato per indicare l'intero sistema operativo, incluse le applicazioni.

Login
La procedura che permette all'utente di accedere a un computer o rete.

Logout
Procedura per chiudere una sessione Linux interattiva.

Memoria principale
Memoria fisica che permette accesso random. Spesso si utilizza il termine RAM (Random Access Memory).

Manpage
Nei sistemi UNIX, la documentazione si trova tradizionalmente nelle manpage o pagine di manuale, alle quali si accede con il comando `man`.

MBR (master boot record)
Il primo settore fisico del disco rigido, il cui contenuto è caricato nella memoria principale ed eseguito dal BIOS. Questo codice carica poi il sistema operativo da una partizione del disco rigido o da un bootloader più sofisticato, come LILO o GRUB.

MD5
Un algoritmo che genera valori hash (somme di controllo MD5 di un file).

Mount
L'inserimento di un file system nell'albero delle directory di un sistema.

MP3
Efficientissima procedura di compressione dei file musicali che li riduce ad un decimo dello spazio occupato dai file non compressi.

Multitasking
I sistemi operativi che possono eseguire contemporaneamente più di un programma vengono chiamati sistemi multitasking (task = compito).

Multiutente
Un sistema al quale possono lavorare contemporaneamente più utenti.

Rete
Collegamento di vari computers per realizzare uno scambio di dati tra loro. Un computer che invia delle richieste via rete viene chiamato anche client, ed il computer che risponse alle richieste server.

NFS (network file system)
Protocollo che permette di accedere ai file system di computer collegati in rete.

NIS (Network Information Service)
Sistema centralizzato di gestione dei dati delle reti (ad esempio, degli username e delle password).

Sistema operativo
Si veda kernel.

Partizione
Sezioni di un disco rigido e ciascuna dotata di un proprio file system o spazio swap.

Path
Descrizione univoca della posizione di un file nel file system.

Plug and Play
Protocollo per il rilevamento e configurazione in automatico.

Processo
Si definisce processo ogni programma o applicazione in corso di esecuzione. Un processo può essere seguito in una shell, immettendo, ad esempio, il comando `top`. Il termine "processo" viene talvolta usato come sinonimo di task (compito).

Processore
Il processore è il cervello di un computer; esso comprende ed elabora i comandi impartiti dall'utente o da un programma. Il processore detiene il controllo dell'intero sistema ed è responsabile delle prestazioni del computer.

Prompt
Breve stringa (configurabile) emessa all'inizio di una linea di comando. Di solito contiene l'attuale directory in cui si lavora.

Protocollo
Standard ideato appositamente per regolare le comunicazioni a livello dihardware, software o di rete. Gli standard più comuni sono HTTP e FTP.

Proxy
: Una memoria intermedia solitamente offerta dai gestori di servizi Internet. Su questa memoria si trova una banca di dati frequentemente richiesti dagli host di una rete. Questa scorciatoia riduce i tempi di scaricamento delle pagine e allegerisce la trasmissione.

RAM (Random Access Memory)
: Vd. Memoria principale

ReiserFS
: Un file system che protocolla le sue modifiche in un cosiddetto "journal". Così, al contrario di Ext2, questo file system può essere ripristinato velocemente. ReiserFS è studiato appositamente per piccoli file.

Root
: L'account del superutente con tutti i permessi. L'account viene utilizzato per interventi di natura amministrativa e non dovrebbe venir utilizzato per mansioni comuni.

Root directory
: La directory "radice" del file system. Essa contiene tutte le altre directory del file system. Su UNIX, la root directory viene anche simbolizzata dal carattere `/`.

SCSI (Small Computer Systems Interface)
: Standard per connettere dischi rigidi e altri dispositivi, come scanner e dispositivi a nastro.

Server
: Un server è solitamente un computer molto capace che fornisce dati e servizi ad altri computer a lui connessi in rete, tipo HTTP, DNS e FTP.

Shell
: Una riga di comando particolarmente flessibile, spesso dotata di uno specifico linguaggio di programmazione. Esempi di shell sono bash, zsh e tcsh.

SMTP (Simple Mail Transfer Protocol)
: Protocollo per la trasmissione della posta elettronica.

SSL (Secure Socket Layer)
Procedura di criptaggio della trasmissione di dati in formato HTTP.

Superuser (super user)
Vd. root.

Amministratore di sistema
Vd. root.

Task
Vd. processo.

TCP/IP
Protocollo di comunicazione utilizzato per l'Internet, spesso usato anche dalle reti.

Telnet
Telnet è un protocolloper la comunicazione tra computer connessi in rete (host) Per login remoto si consiglia di utilizzare comunque SSH, che offre connessioni criptate.

Terminale
Originariamente, un terminale era una combinazione tastiera/schermo allacciata ad un processore centrale, ma priva di una memoria propria. Anche nota con il nome di "workstation" o "postazione". La parola terminale viene oggi usata anche descrivere i programmi che emulano un terminale vero e proprio.

Tux
Il nome del pinguino di Linux (vd. `http://www.sjbaker.org/tux/`).

UNIX
UNIX è (un marchio e) un sistema operativo.

URL (Uniform Resource Locator)
Indirizzo univoco di un sito Internet che contiene il tipo di protocollo (p.es. `http://`) e il nome di un host (p.e. `www.suse.de`) e un documento (p.es., `/us/company/index.html`). Quindi un URL completa sarebbe: `http://www.suse.de/us/company/index.html`.

Directory utente
Vd. directory home.

VESA (Video Electronics Standard Association)
Consorzio industriale che definisce, tra le altre cose, importanti standard di rappresentazione video.

Wildcard
Segnaposto per un (?) o più (*) caratteri. Fanno parte di espressioni regolari.

Window manager
Un window manager è il programma che interagisce tra l'X Window System e l'utente. È responsabile, tra le altre cose, della visualizzazione del desktop. Vi sono molti tipi di window manager e l'aspetto si lascia personalizzare da parte dell'utente.

WWW (World Wide Web)
Basato sul protocollo HTTP; si tratta di una marea di documenti file e immagini visualizzabili tramite browser.

X Window System
L'X Window System è un sistema window basato su rete che gira su tutta una serie di computer; si tratta dello strato tra hardware e window manager.

X11
Versione 11 di X Window System

YaST (Yet another Setup Tool)
L'assistente di sistema di SUSE LINUX.

YP (yellow pages)
Vd. NIS

Indice analitico

C

D

E

F

G

H

I

N

O

P

R

S

T

U

V

W

X

Y