SUSE LINUX

MANUALE DI AMMINISTRAZIONE

3. Edizione 2004

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

traduttori: A B, C D, E F, G H

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

formato: Manuela Piotrowski, Thomas Schraitle

composizione: DocBook-XML und LaTeX

Questo manuale è stato stampato su carta sbiancata senza cloro.

Indice

Benvenuti

Il Administrationshandbuch SUSE LINUX fa luce sulle nozioni fondamentali riguardanti il funzionamento del vostro sistema SUSE LINUX. Trattando i fondamenti dei file system, la configurazione del kernel ed i processi di avviamento, l'allestimento di un server web Apache e l'implementazione di un processo di autenticazione sicuro, questo manuale vi introduce nell'amministrazione di un sistema Linux.

Il Administrationshandbuch SUSE LINUX si compone di cinque maggiori sezioni:

Installazione Illustrazione dettagliata dei diversi modi di eseguire l'installazione, del processo di aggiornamento (update), dei LVM (Logical Volume Manager) e di RAID...

Configurazione Verrà trattata la configurazione del boot loader e del sistema X window, del processo di stampa e dei portatili sotto Linux ...

Sistema Caratteristiche particolari di un sistema SUSE LINUX, dettagli riguardanti il kernel, il concetto di boot ed il processo di inizializzazione ...

Rete Integrazione in reti (eterogenee), installazione e configurazione di un server web Apache, sincronizzazione dei file ed illustrazione di aspetti inerenti alla sicurezza...

Appendice I file system e le ACL (Access Control List)

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

Novità nel Manuale di amministrazione

Ecco le novità rispetto alla versione precedente (SUSE LINUX 9.0) sotto il profilo della documentazione:

- Nel capitolo *Bluetooth – connessione wireless* è stata aggiunta una dettagliata sezione dedicata all'utilizzo di bluetooth (cfr. la sezione 8.4 a pagina 218).
- Il capitolo incentrato sul *power management* è stato arricchito di illustrazioni riguardanti il pacchetto powersave (cfr. sezioni 9.5 a pagina 238 e 9.6 a pagina 244.
- Nel capitolo *Il server web Apache* è stata inclusa una sezione dedicata a Apache 2 (cfr. capitolo 15 a pagina 385).
- Nel capitolo dedicato a *Samba* vi è anche una sezione incentrata su Samba 3 (cfr. capitolo 17.1 a pagina 434).
- Nel capitolo dedicato al processo di stampa sotto Linux è stato posto l'accento sul sistema di stampa CUPS (cfr. capitolo 5 a pagina 93).
- Al capitolo intitolato *X Window System* è stata aggiunta una sezione che tratta in modo dettagliato l'utilizzo di font sotto SUSE LINUX (cfr. la sezione 4.2 a pagina 84).

Convenzioni tipografiche

Nel presente manuale vengono utilizzate le seguenti convenzioni tipografiche:

- YaST

  L'indicazione di un nome di un programma.
- `/etc/passwd`: un file o una directory.
- ⟨*segnaposto*⟩: la sequenza dei caratteri ⟨*segnaposto*⟩ da sostituire con il valore effettivo.
- `PATH`: una variabile di ambiente di nome PATH
- `ls`: comandi.

- `--help`: opzioni e parametri
- `user`: utente.
- (Alt): tasto da premere.
- ‘File’: voci di menu, pulsanti
- "Process killed": comunicazioni di sistema

Allori

E’ l’impegno volontario degli sviluppatori Linux che collaborando a livello mondiale conducono Linux continuamente verso nuovi traguardi. Li ringraziamo per il loro impegno – senza di loro non ci sarebbe questa distribuzione. Grazie anche a Frank Zappa e Pawar.

E chiaramente, last but not least un nostro ringraziamento particolare va a LINUS TORVALDS!

Have a lot of fun!

Il vostro SUSE Team

Parte I

Installazione

L'installazione

SUSE LINUX si lascia installare in modo flessibile; potrete eseguire l'installazione in modo grafico o nel modo testuale che vi permetterà di eseguire numerosi adattamenti.

In questo capitolo troverete una descrizione delle diverse possibilità di installazione, ed indicazioni riguardanti il ricorso a diversi mezzi di installazione (CD-Rom, NFS). Infine, il capitolo vi darà dei consigli su come evitare l'insorgere dei più frequenti problemi d'installazione e su come risoverli. E per concludere vi è una sezione dedicata al partizionamento.

Nota

Nel presente manuale saranno descritte solamente particolari varianti di installazione. Una descrizione dettagliata della installazione standard in modo grafico la trovate all'inizio del manuale dell'utente.

Nota

1.1 L'installazione in modo testo con YaST

1.1.1 Premessa

Oltre all'installazione tramite l'interfaccia grafica, SUSE LINUX può essere installato nel modo testo con YaST (modo di console). Tutti i moduli di YaST sono disponibili anche nel modo testo. Il modo 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. Chiaramente anche i non-vedenti (che dipendono da un'interfaccia testuale) useranno il modo testo.

1.1.2 La schermata di avvio

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 YaST *non* venga avviato automaticamente. Nella riga `boot options` inserite i parametri di caricamento (se il vostro hardware li richiede. Normalmente non ne sussiste la necessità). Con il parametro `textmode=1` potete forzare l'utilizzo del modo testo di YaST. Non dimenticate che durante questa fase iniziale dell'avvio si ha la mappatura americana dei tasti.

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 (Return). Appare ora un dialogo che vi mostra lo stato di progressione

`Loading Linux kernel`; poi, si avvia il kernel e linuxrc. Il programma linuxrc si basa su menù e attende l'immissione di comandi da parte dell'utente.

Problemi possibili

- 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'.
- Se il lettore dei CD-ROM (ATAPI), non funziona come dovrebbe al boot del sistema, consultate la sezione 1.5 a pagina 23.
- Nel caso di difficoltà dovute ad ACPI *Advanced Configuration and Power Interface* disponete dei seguenti parametri del kernel:

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

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

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

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

  Cfr. anche l'articolo della banca dati di supporto: `http://portal.suse.de/sdb/en/2002/10/81_acpi.html`.

- 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 perfetti! Per maggiori approfondimenti, consultate: `http://portal.suse.de/sdb/de/2000/11/thallma_memtest86.html`

  Si consiglia di eseguire il test della memoria durante la notte.

1.1.3 La base: linuxrc

Con il programma linuxrc, potete eseguire le impostazioni per l'installazione nonché caricare i driver come moduli del kernel. Alla fine, linuxrc avvierà il programma d'installazione YaST che darà inizio all'installazione vera e propria del software di sistema e dei programmi.

Con ↑ e ↓ selezionate le voci di menù e con ← e → i comandi come 'Ok' o 'Interrompi'. Per una descrizione più dettagliata di linuxrc, consultate la sezione 12.4 a pagina 278.

Impostazioni

Il programma linuxrc inizia automaticamente con la selezione della lingua e della tastiera.

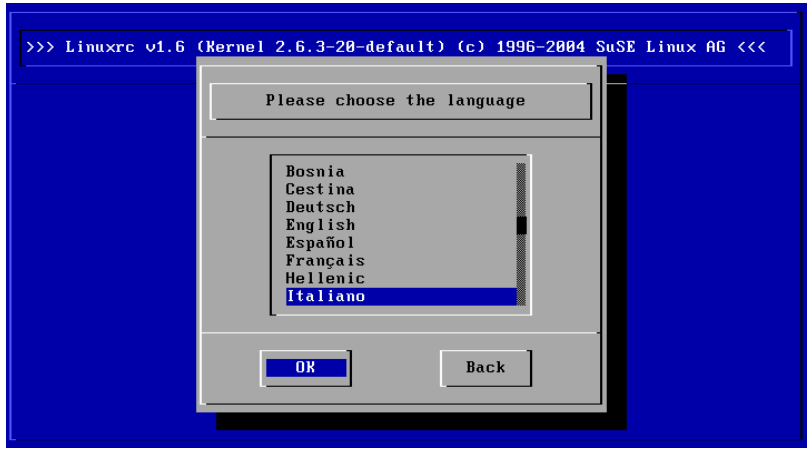

Figura 1.1: *Scelta della lingua*

- Selezionate la lingua dell'installazione (ad esempio, 'Italiano') e confermate con Return .
- Selezionate poi la mappatura della tastiera (p.es. 'Italiano').

Problemi possibili

- linuxrc non offre la mappatura della tastiera richiesta. In tal caso, scegliete intanto un'alternativa (per esempio, 'English (US)'); dopo

l'installazione, potrete passare alla mappatura da voi richiesta con YaST.

Menù principale di linuxrc

Ci troviamo ora nel menù principale di linuxrc (Figura 1.2).

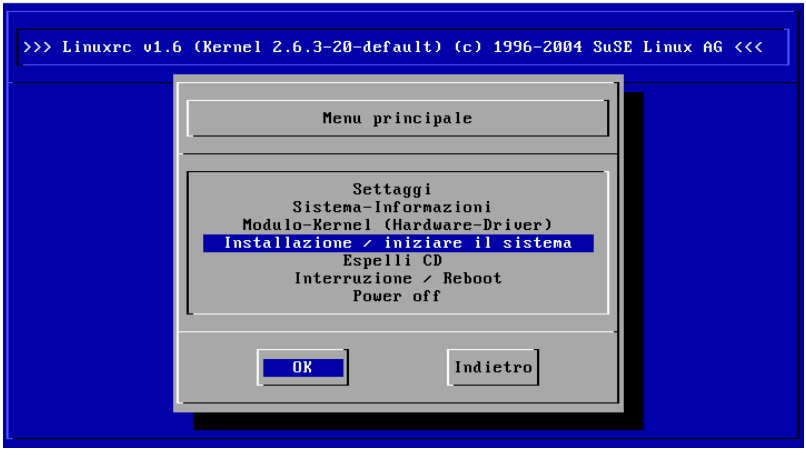

Figura 1.2: *Menu principale di linuxrc*

Questo menù vi offre le seguenti opzioni:

'Settaggi' Scegliete la lingua, il monitor e la tastiera, come descritto sopra.

'Sistema-Informazioni' Qui trovate le informazioni sull'hardware, a condizione che sia stato rilevato dal kernel o che venga già indirizzato dai moduli caricati.

'Modulo-Kernel (Hardware-Driver)'
Se necessario, caricate i moduli corrispondenti all'hardware. In questo menù trovate anche una serie di file system che potrete caricare in aggiunta, come ad esempio ReiserFS.

Di solito *non* bisogna selezionare questa voce, se il vostro disco rigido (o i dischi) ed il vostro lettore CD-ROM (ATAPI) sono entrambi collegati ad un controller (E)IDE, dal momento che il kernel contiene un proprio supporto (E)IDE. Per maggiori dettagli sulla scelta dei moduli vedi la sezione seguente.

'Avvia installazione/sistema' Con questo punto, si passa all'installazione vera e propria.

'Interruzione/Reboot' In caso cambiate idea…

'Power off' Per fermare il sistema e spegnerlo.

Integrazione dell'hardware tramite moduli

Selezionate i moduli del kernel da caricare alla voce 'Moduli kernel', quando vi serve il supporto per particolari caratteristiche del sistema: generalmente, si tratta di componenti SCSI, schede di rete o PCMCIA o di lettori CD-Rom *non* ATAPI. Alcuni driver adesso li trovate solo sotto forma di moduli che potrete caricare all'occorrenza (p.es. IDE) , altri sono stati aggiunti al kernel (p.es. USB, FireWire o file system).

Per sapere di più sul caricamento dei moduli, leggete la sezione 12.4 a pagina 278. Nel sottomenù successivo, selezionate il motivo per il quale volete o dovete caricare i moduli, per esempio:

Un modulo per SCSI se avete un disco rigido SCSI o un lettore CD-Rom SCSI.

Un modulo per CD-Rom se il vostro lettore CD-Rom *non* è connesso ad un controller (E)IDE o SCSI. Questo è spesso il caso per lettori CD-Rom datati connessi al computer tramite un controller proprietario.

Un modulo per la rete se volete eseguire l'installazione tramite NFS o FTP. Per maggiori dettagli, vd. la sezione 1.3.2 a pagina 17.

Uno o più file system come ad es. ReiserFS o ext3.

Nota

Se tra i moduli standard non trovate il driver adattato per il vostro dispositivo di installazione (lettore CD-Rom proprietario o su porta parallela, scheda di rete, PCMCIA), potrete ricorrere anche ai driver che trovate sul dischetto dei moduli; per creare un dischetto del genere vd. 1.4 a pagina 18. Andate alla fine dell'elenco e selezionate la voce 'Altri moduli'; in questo caso, linuxrc vi chiederà il dischetto dei moduli.

Nota

Avviare l'installazione

Dal momento che solitamente avete già selezionato 'Avvia installazione/sistema', basta ora premere Return per passare all'installazione vera e propria.

Figura 1.3: *Menu di installazione di linuxrc*

Potete scegliere tra i seguenti punti:

'Iniziare l'installazione' Probabilmente, quello che siete in procinto di fare.

'Fare il boot del sistema installato'
Ne avrete forse bisogno più tardi, in caso si verifichino dei problemi dovuti al boot loader.

'Iniziare il sistema dell' aiuto' Questa opzione vi aiuterà nel caso si verifichino dei problemi con il sistema installato.

Per passare all'installazione, premete Return per la voce 'Avvia installazione/update'. Scegliete ora il mezzo sorgente: normalmente basta lasciare il cursore sulla voce preselezionata: 'CD-ROM'.

Premete ora Return. L'ambiente di installazione viene avviato direttamente dal CD 1 o DVD. Non appena questo processo è concluso parte YaST nel modo di testo (ncurses). L'installazione ha inizio.

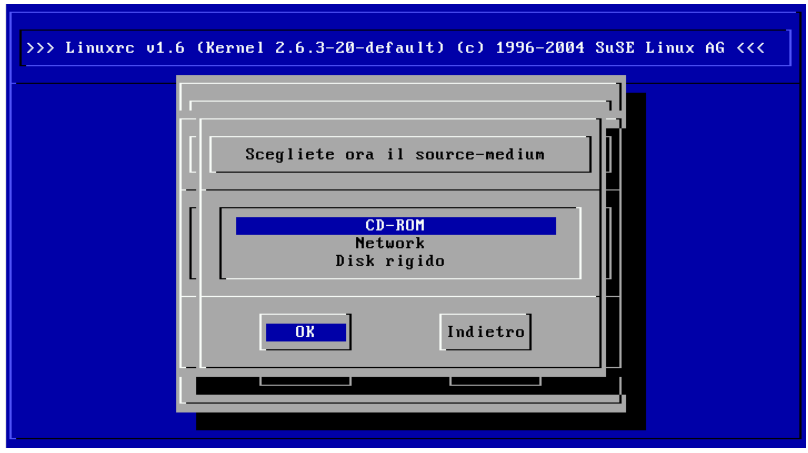

Figura 1.4: *Selezione del mezzo sorgente su linuxrc*

Possibili difficoltà

- L'adattatore SCSI non viene riconosciuto:
  - Provate a caricare il modulo di un driver compatibile.
  - Usate un kernel con un driver SCSI integrato; un kernel del genere lo dovete compilare voi.
- Il lettore CD-ROM ATAPI si blocca in fase di lettura: vd. sezione 1.5 a pagina 23.
- Eventualmente si possono verificare delle difficoltà durante il caricamento dei dati nella ram-disk, in modo che risulti impossibile caricare YaST. Nella maggior parte dei casi, il seguente procedimento porta ad un risultato accettabile:

  Selezionate, nel menù principale di linuxrc, 'Impostazioni' -> 'Debug (Esperti)'; impostate 'Forza root image' (*Force root image*) su 'no'. Tornate al menù principale e ricominciate l'installazione da capo.

1.2 Avviare SuSE Linux

Dopo aver eseguito l'installazione resta da chiarire in che modo desiderate avviare Linux nell'uso quotidiano. Segue una rassegna delle diverse pos-

sibilità per caricare Linux; quali di questi metodi sia il più indicato per voi dipende soprattutto da quello che intendete fare.

Dischetto di avvio Inizializzate Linux con il *dischetto di avvio*. Questa possibilità funziona sempre e non crea problemi - - il dischetto di avvio può venir creato con YaST; cfr. [1], capitolo *YaST – configurazione*, sezione *Creare dischetto di avvio, ripristino e dei moduli*.

Il dischetto di avvio è una buona soluzione intermedia se non riuscite ancora a configurare le altre possibilità o se volete rinviare la decisione definitiva riguardante l'uso del meccanismo di avvio. L'uso del dischetto per il boot può essere una buona soluzione anche quando non volete sovrascrivere il boot loader di un altro sistema operativo.

Linux Bootloader La soluzione migliore da un punto di vista tecnico è l'utilizzo di un boot manager Linux, come LILO (LInux LOader) o GRUB, che vi permette di scegliere al boot tra i diversi sistemi operativi. Il bootloader si lascia configurare già durante l'installazione o in un secondo momento p.es. tramite YaST.

Attenzione

Ci sono varianti del BIOS, che controllano la struttura del Master Boot Record (MBR), e dopo una installazione di LILO riportano erroneamente un avviso di virus. Questo problema si può evitare disabilitando il controllo dei virus nel BIOS (dovete disabilitare 'virus protection'). – Più tardi potrete riattivare questa opzione; essa è però superflua se usate esclusivamente Linux come sistema operativo.

Attenzione

Troverete una descrizione dettagliata dei diversi metodi per il boot, specialmente per ciò che riguarda GRUB e LILO, nel capitolo 7 a pagina 177 ss.

1.2.1 La schermata grafica di SUSE

Da SUSE LINUX 7.2 sulla console 1 viene visualizzata la schermata grafica di SUSE, se quale parametro del kernel è attivata l'opzione "vga=<valore>"; durante l'installazione con YaST questa opzione viene rilevata automaticamente in base alla risoluzione scelta e la scheda grafica utilizzata.

Disattivare la schermata SUSE

In linea di massima avete tre possibilità:

- disattivare la schermata all'occorrenza immettendo sulla riga di comando `echo 0 >/proc/splash`.

  e il seguente comando per riattivarla `echo 0x0f01 >/proc/splash`.

- disattivare la schermata di default:

  Aggiungete un parametro del kernel `splash=0` alla configurazione del bootloader. Nel capitolo 7 a pagina 177 troverete delle informazioni dettagliate. Se preferite comunque il modo testo, lo standard nella versioni precedenti, impostate `"vga=normal"`.

- disattivare la schermata una volta per tutte:

  Compilate un nuovo kernel e disattivate l'opzione 'Use splash screen instead of boot logo' nel menu 'frame-buffer support'.

Nota

Se avete disattivato il supporto frame buffer nel kernel, avete automaticamente disattivato anche lo splash-screen. Se compilate un kernel proprio, SUSE non vi può garantire alcun supporto a riguardo!

Nota

1.3 Installazioni particolari

1.3.1 Installazione senza supporto di CD-ROM

Cosa fare, se un'installazione tramite CD-ROM non è possibile? Potrebbe per esempio darsi il caso che il vostro lettore di CD-ROM non sia più supportato, perché si tratta di un'unità disco un pò antiquata e proprietario. Oppure, eventualmente, non avete sul vostro secondo computer (p.e. un portatile) un lettore di CD-ROM, ma avete in compenso un adattatore Ethernet.

SUSE LINUX può essere installato su computer senza supporto per CD-Rom tramite un collegamento di rete: solitamente si ricorrerà a NFS o FTP via Ethernet, come descritto di seguito.

1.3.2 Installazione tramite rete

Per questo metodo non è possibile richiedere il supporto all'installazione. Questo metodo d'installazione dovrebbe venire eseguito solo da esperti. Per installare SUSE LINUX da una sorgente di installazione che si trova nella rete dovete eseguire i seguenti passi:

1. Rendere disponibili i dati da installare (CD, DVD) su un computer che sarà la sorgente dalla quale verrà installato SUSE LINUX.
2. Avviare il sistema da installare tramite dischetto o CD e configurare la rete.

Creare una sorgente di installazione nella rete

Create le share di rete copiando il CD di installazione in singole directory e mettetele su un sistema che funge da server NFS. Per quanto riguarda computer su cui gira SUSE LINUX potete copiare ogni CD p.es. con il seguente comando: `cp -a /mnt/cdrom /suse-share/`. Cambiate in seguito il nome della directory (p.es. CD1): `mv /suse-share/cdrom /suse-share/CD1`.

Ripetete il procedimento anche per gli altri CD. Per concludere consentite l'accesso alla directory `/suse-share` tramite NFS; cfr.sezione 14.9 a pagina 371.

L'avvio per l'installazione via rete

Inserite il mezzo di avvio (dischetto, CD-Rom) nell'apposita unità; come creare un dischetto di avvio viene spiegato nelle sezioni 1.4.1 nella pagina successiva e 1.4.2 a pagina 20. Dopo un pò, apparirà il menu di avvio. Selezionate qui 'Installazione manuale'. Potete anche immettere altri parametri del kernel. Confermate con Enter. Il kernel viene caricato e vi sarà chiesto di inserire il dischetto dei moduli.

Quindi appare linuxrc e vi chiede di immettere dei parametri:

1. Selezionate la lingua ed eventual. la mappatura della tastiera in linuxrc.
2. Selezionate 'Moduli del kernel (driver hardware)'.
3. Caricate eventualmente i driver IDE, RAID o SCSI necessari per il vostro sistema.

4. Selezionate ‘Carica driver di rete’ e caricate il driver di rete che vi serve (p.es. `eepro100`).
5. Selezionate ‘Carica driver del file system’ e caricate i driver richiesti (p.es. `reiserfs`).
6. Selezionate ‘Indietro’ ed infine ‘Avvia installazione / sistema’.
7. Selezionate ‘Avvia installazione / update’.
8. Selezionate ‘Rete’ e poi come protocollo di rete p.es. `NFS`.
9. Selezionate la scheda di rete che volete usare.
10. Immettete gli indirizzi IP e gli altri dati di rete.
11. Immettete l’indirizzo IP del server NFS che mette a disposizione i dati da installare.
12. Immettete il percorso per le share NFS (p.es. `/suse-share/CD1`).

linuxrc a questo punto carica l’ambiente di installazione dalla sorgente nella rete ed infine YaST. Concludete l’installazione come descritto in [1], capitolo *Installazione*.

Possibili difficoltà

- L’installazione si interrompe prima che sia veramente cominciata: l’indirizzario d’installazione dell’ altro computer non è stato esportato assieme ai diritti `exec` – provvedete.
- Il server non riconosce il computer su cui volete installare SUSE LINUX. Aggiungete il nome e l’indirizzo IP del nuovo computer nel file `/etc/hosts` sul server.

1.4 Consigli e trucchetti

1.4.1 Creare un dischetto di avvio sotto DOS

Premesse

Vi serve un dischetto 3.5 HD, ovvero ad alta densità, formattato e un lettore floppy 3.5 capace di eseguire il boot.

Informazioni aggiuntive

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.

Procedimento

Per creare i dischetti di caricamento e dei moduli SUSE, ci si serve del programma DOS rawrite.exe (CD 1, directory `dosutils\rawrite/`). Avrete bisogno di un PC con DOS (ad esempio, FreeDOS) o Windows.

Descriveremo ora i singoli passi da seguire se utilizzate Windows:

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:`

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

4. Dopo l'avvio, il programma vi chiede la sorgente *source* e la destinazione *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, alla directory `boot/`. Il file si chiama semplicemente `bootdisk`. Non dimenticate di indicare il percorso per il vostro lettore di CD!

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

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

Dopo aver inserito il lettore di destinazione `a:`, il programma rawrite vi invita ad inserire un dischetto formattato e a premere il tasto Enter. Il processo di copiatura dei dati verrà protocollato in modo dettagliato. Per interromperlo, premete la combinazione di tasti Ctrl + c.

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 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.

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

Premessa

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
   ```

2. Eseguite il mount del CD 1, ad esempio, su `/media/cdrom`:

   ```
   mount -tiso9660 /dev/cdrom /media/cdrom
   ```

3. Andate nella directory `boot` sul CD:

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

4. Ora create il dischetto di avvio con

   ```
   dd if=/media/cdrom/boot/bootdisk of=/dev/fd0 bs=8k
   ```

   Il file `LEGGIMI` ovvero `README` nella directory `boot`, vi dà la possibilità di approfondire il tema 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` e `modules2` `modules3` e `modules4`. Ne avrete bisogno se avete dei dispositivi SCSI o 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.

Un po' più complesso è il caso in cui, per esempio, vogliate utilizzare un kernel da voi stesso compilato durante l'installazione; in questo caso memorizzate l'immagine standard (`bootdisk`) sul dischetto e sovrascrivete poi il kernel in essa contenuto (`linux`) con il vostro (cfr. sezione 11.6 a pagina 261):

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

1.4.3 Avvio dal dischetto (SYSLINUX)

Il cosiddetto il dischetto di avvio viene usato in circostanze particolari durante l'installazione (ad esempio, quando il PC non dispone di un lettore di CD-ROM). Per creare un tale dischetto vi preghiamo di consultare 1.4.1 a pagina 18 oppure 1.4.2 nella pagina precedente.

Il processo di avvio ovvero di boot viene inizializzato dal boot loader SYSLINUX (il `syslinux`). SYSLINUX è configurato in modo tale da non eseguire un rilevamento completo dell'hardware durante l'avvio. Essenzialmente, esso esegue i seguenti processi:

- Controlla se il BIOS offre supporto per il framebuffer secondo lo standard VESA 2.0 e carica di conseguenza il kernel.
- Legge i dati del monitor (informazioni DDC).
- 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 veder se il BIOS supporti tali funzioni.

Nota

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 comunicherà quale azione sta eseguendo.

Nota

Possibili difficoltà

- 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`

1.4.4 Caricare il sistema dal CD 2

Potrete 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 MB. 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).

1.4.5 Linux supporta il mio CD-ROM-drive?

In generale, si può dire che la maggioranza dei lettori di CD-ROM è supportata.

- Con unità ATAPI non dovrebbero verificarsi dei problemi.
- Con drive CD-ROM SCSI tutto dipende dal supporto per il controller SCSI al quale è collegato il lettore CD-ROM. Nella banca dati dei componenti CDB trovate l'elenco dei controller SCSI supportati. Se il vostro controller SCSI non è supportato e, in più, al controller è collegato anche il disco rigido, avete in ogni caso un problema…
- Anche molti drive CD-ROM non standardizzati funzionano con Linux, anche se non si può escludere il verificarsi di difficoltà. Se il vostro drive non è esplicitamente incluso nell'elenco, provate con un tipo simile dello stesso produttore.

- Vengono supportati anche lettori di CD-ROM USB. Se il BIOS del vostro computer non supporta ancora l'avvio di dispositivi USB, dovete iniziare l'installazione tramite un dischetto di avvio. Per maggiori dettagli vedi 1.4.3 a pagina 21. Prima di eseguire l'avvio dal dischetto accertatevi che gli dispositivi USB siano collegati e accesi.

1.5 Il CD-ROM ATAPI si inceppa durante la lettura

Se il dispositivo ATAPI CD-ROM non viene riconosciuto o si inceppa durante la lettura, ciò è dovuto al fatto che l'hardware non è impostato nel modo giusto. Normalmente, ogni dispositivo dovrebbe essere collegato secondo un preciso ordine all'(E)IDE-Bus, ovvero: il primo dispositivo è master sul primo controller, il secondo è slave; il terzo dispositivo è master sul secondo controller e il quarto è slave.

Spesso capita che in un computer ci sia, assieme al disco rigido, solo un lettore per il CD-ROM e che questo sia collegato come master al secondo controller. In alcuni casi del genere, Linux non riesce a rilevarlo; quasi sempre, si può aiutare il kernel indicandogli un parametro corrispondente (`hdc=cdrom`).

Qualche volta succede anche che un dispositivo sia semplicemente collegato in maniera sbagliata, vale a dire: è configurato come slave ma è collegato come master al secondo controller o viceversa. Se avete dei dubbi, controllate queste impostazioni e, se necessario, correggetele.

Esistono, inoltre, una serie di chip set EIDE difettosi; nonstante ciò la maggioranza di essi viene riconosciuta e il kernel contiene codici per evitare problemi. Per questi casi, esiste un kernel speciale; (cfr. il `README` in `/boot` del CD-ROM d'installazione).

Se il boot non funziona subito, provate con i seguenti parametri del kernel:

`hdx=cdrom` `x` sta qui per `a`, `b`, `c`, `d` etc. e va interpretato come segue:

- `a` – master al 1. controller IDE
- `b` – slave al 1. controller IDE
- `c` – master a 2. controller IDE
- …

Esempio di `parametri_da_immettere`: `hdb=cdrom` con questo parametro indicate il CD-ROM drive al kernel – in caso non lo trovi da sé – e siete in possesso di un CD-ROM drive ATAPI collegato come slave al primo IDE controller.

`idex=noautotune` `x` sta per `0`, `1`, `2`, `3` etc. e va interpretato come segue:

- `0` – 1. controller IDE
- `1` – 2. controller IDE
- …

Esempio di `parametri_da_immettere`: `ide0=noautotune`. Questo parametro è spesso d'aiuto con i dischi rigidi (E)IDE.

1.6 Assegnare ai dispositivi SCSI dei nomi di dispositivo permanenti

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 alla configurazione dei dispositivi ed al 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 delle difficoltà dovute a questa ragione, si dovrebbe utilizzare `boot.scsidev`. `boot.scsidev` configura i dispositivi SCSI, all'avvio e registra dei nomi di dispositivo fissi sotto `/dev/scsi/` da poter utilizzare nel `/etc/fstab`.

Nel modo per esperti dell'editor dei runlevel, `boot.scsidev` va abilitato per il livello `B`, quindi verranno creati i riferimenti necessari in `/etc/init.d/boot.d` per la creazione dei nomi durante il processo di avvio.

1.7 Partizionare per esperti

Nel capitolo sulla installazione standard (si veda [1]) vengono trattate le possibilità di partizionamento del sistema. Questo paragrafo intende fornire informazioni dettagliate con le quali ottenere uno schema di partizione

su misura per le vostre esigenze. Questo paragrafo è di particolare interesse soprattutto per coloro che vogliono configurare il proprio sistema in modo ottimale – sia per quanto riguarda la sicurezza che la velocità – e sono disposti a reinstallare il sistema; fare, per così dire, tabula rasa.

È assolutamente necessario avere cognizioni di base sul funzionamento di un file system di UNIX e non dovrebbero esservi sconosciuti concetti come punto di mount, partizioni fisiche, partizioni estese o partizioni logiche.

Per prima cosa dovete raccogliere le seguenti informazioni:

- In quale ambito volete usare il computer (server di file, server delle applicazioni, postazione di lavoro)?
- Quante persone lavoreranno su questo computer (login simultanei)?
- Quanti hard disk ha il computer, che capacità hanno e di che tipo sono (controller EIDE, SCSI o RAID)?

1.7.1 Dimensione della partizione swap

Spesso leggerete come minimo lo spazio di swap deve corrispondere al doppio della memoria RAM. Questa formula è un lascito dei tempi in cui 8 MB di RAM nel computer erano un lusso di pochi; Un computer dovrebbe disporre ca. 30/ 40 MB di memoria virtuale, dunque Ram più swap. Con applicazioni moderne che richiedono molta memoria, bisogna correggere questi valori verso l'alto. Attualmente e per il prossimo futuro un utente medio con 256 MB di memoria virtuale va sul sicuro. Quello che non dovete assolutamente fare è non dedicare alcun spazio alla memoria swap.

1.7.2 Campo d'impiego del computer

Impiego come workstation

Il caso più frequente d'uso di un computer Linux è l'impiego come workstation. Affinché possiate orientarvi a dei valori concreti, abbiamo messo assieme un paio di esempi di configurazione, che potrete adattare a seconda delle vostre necessità. Nella tabella 1.1 nella pagina successiva avete un sommario dei diversi volumi d'installazione per un sistema Linux.

Tabella 1.1: Installazione

Installazione	Spazio richiesto
minima	180 MB fino a 400 MB
piccola	400 MB fino a 1500 MB
media	1500 MB fino a 4 GB
grande	oltre 4 GB

Esempio: computer standard per postazione di lavoro (piccola)

Avete a disposizione sull'hard disk ca. 500 MB e volte installarci Linux: una partizione swap di 64 MB e il resto per `/` (la partizione root).

Esempio: computer standard per postazione di lavoro media

Per Linux avete a disposizione 2 GB. Piccola partizione di boot `/boot` (5-10 MB risp. 1 cilindro) 128 MB di swap, 800 MB per `/` e il resto per una partizione separata `/home`

Esempio: computer standard per una postazione di lavoro di lusso

Se avete a disposizione più di 2 GB, non esiste nessuno standard di partizionamento; vedi la sezione 1.7.3 a fronte.

Impiego come server di file

Qui la performance del vostro hard disk è *veramente* importante e si dovrebbe dare la preferenza a dispositivi SCSI. Fate anche attenzione alle performance dei dischi e dei controller.

Un file server offre la possibilità di gestire i dati centralmente; può trattarsi di home directory degli utenti, di una banca dati o di archivi. Il vantaggio è una amministrazione più semplice. Se il file server troverà impiego in una rete di una certa estensione (a partire da 20 utenti), è essenziale ottimizzare l'accesso al disco rigido. Mettiamo il caso che vogliate impostare un file server Linux che debba consentire l'accesso alle directory home di 25 utenti, e sapete che ogni utente utilizzerà al massimo 100-150 MB per i propri dati personali; allora basterà un disco da 4 GB montato sotto `/home/`, se non tutti gli utenti si mettono a compilare nella propria directory home.

Se avete 50 utenti, dal punto di vista puramente matematico, sarebbe necessario un disco da 8 GB; è però meglio in questi casi dividere `/home/` su

due dischi da 4 GB, poiché questi si possono dividere il carico di lavoro (e il tempo di accesso).

Nota

La memoria cache di un browser web va tenuta assolutamente su hard disk locali!

Nota

Impiego come server di calcolo

Questo tipo di server è solitamente un computer molto potente che in una rete si assume i compiti di calcolo intensivo. Un tale computer dispone tipicamente di una memoria principale un po' più capiente (dai 512 MB di RAM in su). L'unico punto dove bisogna intervenire per assicurare una elevata velocità del disco è rappresentato da eventuali partizioni swap. Anche qui vale la regola: è preferibile suddividere su più dischi le partizioni swap.

1.7.3 Ottimizzazione

I dischi rigidi rappresentano generalmente il cosiddetto "collo di bottiglia". Per aggirarlo, esistono tre possibilità che vanno applicate congiuntamente:

- Dividete il carico di lavoro in parti uguali su più dischi.
- Impiegate un file system ottimizzato (p. e. `reiserfs`).
- Allocate sufficiente memoria (al meno 256 MB) per il vostro file server.

Più dischi in parallelo

Qui è necessaria una spiegazione un po' più dettagliata. Il tempo totale necessario per il trasferimento di dati è dovuto in circa:

1. Al tempo necessario affinché la richiesta arrivi al controller del disco.
2. Al tempo necessario affinché il controller del disco invii questa richiesta all'hard disk.
3. Al tempo necessario affinché l'hard disk posizioni la testina.
4. Al tempo necessario affinché il dispositivo si porti sul settore giusto.
5. Al tempo per il trasferimento dei dati.

Il punto 1 dipende dalla connessione di rete e va regolato in quella sede. Il punto 2 è un intervallo di tempo veramente minimo che dipende dal controller del disco. I punti 3 e 4 rappresentano lo scoglio maggiore. Il posizionamento viene misurato in ms (millesimi di secondo): se guardiamo ai tempi d'accesso (misurati in ns nano-secondi) nella memoria principale, abbiamo un fattore di 1 milione. Il punto 4 dipende dal numero di giri per minuto del disco. Il punto 5 dipende dal numero dei giri e dal numero delle testine, come pure dal posizionamento della testina (interno o esterno).

Per una ottima performance si deve quindi intervenire sul punto 3. Nei dispositivi SCSI entra qui in gioco la funzione disconnect; ecco cosa succede con la suddetta caratteristica:

Il controller manda al dispositivo collegato (in questo caso l'hard disk) il comando Vai alla traccia x, settore y. Ora è la meccanica relativamente lenta del disco che si mette in movimento. Se il disco è intelligente (cioè dispone della funzione disconnect) e se anche il driver per il controller dispone di questa caratteristica, il controller manda al disco subito dopo l'operazione richiesta il comando "disconnect" e il disco si disconette dal bus SCSI. Da questo momento in poi anche gli altri dispositivi SCSI possono portare a termine il loro transfer di dati. Dopo un po' (a seconda della strategia o del carico del bus SCSI) viene riattivato il collegamento con il disco; di solito, a questo punto il dispositivo ha già raggiunto la traccia richiesta.

In un sistema operativo multitasking e multiutente come Linux sono parecchie le ottimizzazioni che si possono attuare. Guardiamo un po' un dettaglio dell'output del comando `df` (cfr. output 1.1).

Exempio 1.1: *Esempio di output del comando df*

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

Quali sono dunque i benefici dell'uso parallelo di più dischi? Facciamo un esempio, immettiamo in `/usr/src`:

```
tar xzf pacchetto.tar.gz -C /usr/lib
```

Ciò significa che pacchetto.tar.gz debba venire installato sotto `/usr/lib/pacchetto`. Per farlo, la shell chiama `tar` e `gzip` (che risiedono sotto `/bin` e quindi su `/dev/sda`), poi viene letto `pacchetto.tar.gz` di `/usr/src` (che si trova su `/dev/sdb`). Infine, i dati estratti vengono scritti sotto `/usr/lib` (che si trova su `/dev/sdc`). Ora sia il posizionamento che l'accesso in lettura/scrittura al buffer interno del disco possono venire eseguiti quasi in parallelo.

Questo è solo un esempio fra tanti. Come regola generale vale che, in presenza di diversi dischi (della stessa velocità), `/usr` e `/usr/lib` dovrebbero risiedere su dischi differenti; `/usr/lib` dovrebbe avere ca. il 70% del volume di `/usr`. La directory root `/` dovrebbe trovarsi sul disco su cui si trova `/usr/lib` per ragioni dovuti alla frequenza di accesso.

Da un certo numero di dischi SCSI in poi (ca. da 4 a 5), si dovrebbe prendere seriamente in considerazione l'acquisto di un controller RAID. Grazie ad esso, le operazioni sui dischi non vengono solo eseguite in modalità quasi-parallela, bensì in modalità parallela reale. La tolleranza agli errori è un ulteriore vantaggio non del tutto secondario.

Velocità del disco e la dimensione della memoria principale

Molto spesso sentirete dire che la dimensione della memoria principale sotto Linux è più importante della velocità del processore. Uno dei motivi - se non il principale - è la capacità di Linux di creare buffer dinamici contenti dei dati dell'hard disk. Per farlo Linux utilizza vari trucchetti, come p.es. read ahead (lettura anticipata) e delayed write (salva diverse operazioni di scrittura per poi eseguirle in una volta sola). Quest'ultima caratteristica è il motivo per cui non si deve mai spegnere un computer Linux in maniera scorretta. Entrambi i fattori sono la spiegazione del fatto perché la memoria principale sembra riempirsi con il tempo, e perché Linux sia così veloce; cfr. anche la sezione 12.2.6 a pagina 271.

1.8 Configurazione dell'LVM con YaST

Con questo tool di partizionamento professionale potrete elaborare e cancellare partizioni esistenti o crearne di nuove. Da qui giungete alla maschera di configurazione di Soft-RAID e LVM.

Nota

Tante utili indicazioni riguardanti il partizionamento si trovano nella sezione 1.7 a pagina 24.

Nota

Di solito il partizionamento viene eseguito durante l'installazione. Se volete integrare un secondo disco rigido, potrete integrarlo anche nel vostro sistema Linux esistente. Dovrete partizionare il nuovo disco rigido, eseguire il mount delle partizioni e registrarle nel file `/etc/fstab`. Potrebbe anche rendersi necessario spostare alcuni dati per trasferire una partizione `/opt/` troppo piccola sul nuovo disco rigido.

Nel caso in cui vogliate modificare le partizioni di un disco rigido con il quale state lavorando, dovrete fare molta attenzione: è possibile, ma dovrete riavviare il sistema subito dopo. Molto più sicuro è modificare le partizioni dopo aver fatto il boot dal CD. Nel partizionatore, accanto al bottone 'Esperti...', troverete un menù a tendina con i seguenti comandi:

Rileggere tabella di partizione Per rileggere le partizioni del vostro disco rigido. Questo è necessario, ad esempio, ogni volta che abbiate partizionato il disco manualmente dalla console di testo.

Usa punti di mount di /etc/fstab attuale
Importante solo durante l'installazione. Far leggere il vecchio `fstab` è richiesto se non eseguite un update, ma una nuova installazione. In questo caso, non avrete bisogno di inserire manualmente i punti di mount.

Cancella tabella di partizione e disk label
Con questo comando, potrete completamente sovrascrivere la vecchia tabella delle partizioni con quella vecchia. Cosa utile, ad esempio, se si verificano dei problemi con label un pò particolari. Con questo metodo, tuttavia, perderete tutti i dati del disco rigido.

1.8.1 Logical Volume Manager (LVM)

A partire della versione 2.6 del Kernel, il Logical Volume Manager (LVM) è a vostra disposizione nella versione 2; è compatibile con la versione precedente e può amministrare vecchi volume group. Se create dei nuovi volume group dovete stabilire se intendete utilizzare il nuovo formato oppure la versione compatibile con quella precedente. LVM2 non richiede delle

kernel patch è utilizza il `device-mapper` integrato nel Kernel 2.6. A partire da questa versione del Kernel può essere utilizzato solo la versione 2 dell'LVM. In questo capitolo quando si parla di LVM si intende sempre la versione 2.

Un'alternativa a LVM2 è rappresentata da EVMS (Enterprise Volume Management System) che offre un'interfaccia per Logical Volume e Raid Volume. EVMS usa alla stregua di LVM2 il device mapper integrato nel Kernel 2.6.

Il Logical Volume Manager (LVM) vi permette di allocare in modo flessibile lo spazio del vostro disco rigido ai diversi file system. Dal momento che non è per niente semplice modificare delle partizioni di un sistema in esecuzione si è pensato di creare l'LVM: esso mette a disposizione un "pool" virtuale (Volume Group) di spazio di memoria, da cui, attingere in caso di necessità, per creare dei logical volume. Il sistema operativo accede a questi volumi logici, anzicché a delle partizioni fisiche.

Particolarità:

- Più dischi rigidi/partizioni possono essere riuniti in un unica grande partizione.
- 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.
- Più dischi rigidi possono essere utilizzati nel modo RAID 0 (striping) che comporta una migliore prestazione.
- Il feature "snapshot" consente soprattutto con server, di ottenere dei backup consistenti con il sistema in esecuzione.

L'impiego dell'LVM conviene anche su un PC privato 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 del LVM ufficiale `http://tldp.org/HOWTO/LVM-HOWTO/`.

Configurazione dell'LVM con YaST

Per preparare la configurazione dell'LVM con YaST, create una partizione LVM durante l'installazione: nella schermata in cui vi vengono proposte delle partizioni, cliccate su 'Partizionamento'; nella schermata che segue, selezionate poi 'Rifiuta' o 'Modifica'. Ora, dovete creare una partizione per l'LVM: nel partizionatore, selezionando 'Crea' -> 'Non formattare' e cliccando sulla voce '0x8e Linux LVM'. Potete concludere il partizionamento con l'LVM subito o in un secondo momento, ad installazione del sistema avvenuta. In quest'ultimo caso, evidenziate la partizione LVM nel partizionatore e cliccate su 'LVM...'.

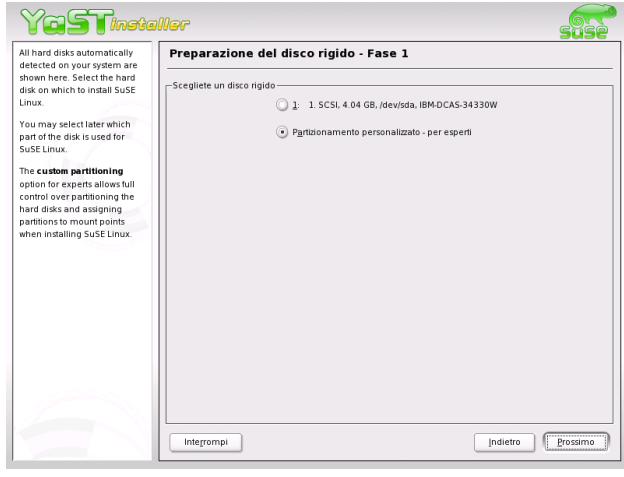

Figura 1.5: *YaST: attivare LVM durante l'installazione*

LVM – Il partizionatore

Dopo aver selezionato 'LVM...', la prima cosa che vedrete è un dialogo, tramite il quale potrete modificare le partizioni del vostro disco rigido. Potrete naturalmente anche crearne di nuove. La partizione per l'LVM dovrà ricevere il codice di identificazione 8E. Queste partizioni sono accompagnate dalla indicazione "Linux LVM", nella lista delle partizioni della finestra (vd. ultima parte).

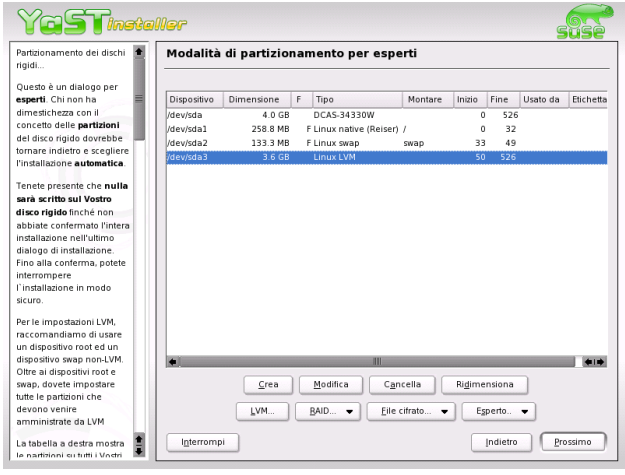

Figura 1.6: *YaST: il partizionatore*

Nota

Ripartizionare i Logical Volume

All'inizio dei PV vengono scritti delle informazioni riguardante il volume nella partizione. In tal maniera un PV "sa" a quale Volume Group appartiene. Se volete modificare la partizione si consiglia di cancellare l'inizio del volume. Nel caso di un Volume Group "system" e di un Physical Volume /dev/sda2 potete farlo p.es. con il comando `dd if=/dev/zero of=/dev/sda2 bs=512 count=1`.

Nota

Non è necessario impostare tutte le partizioni previste per l'LVM, una per una, sul codice di partizione `8E`. Se necessario, YaST imposterà il codice di una partizione dedicata ad un Volume Group LVM automaticamente su `8E`. Se, sul vostro disco, dovessero esservi dei settori non partizionati, create delle partizioni LVM per tutte le aree disponibili servendovi di questo dialogo. Impostate queste partizioni subito su `8E`, non dovrete formattarle in seguito, e non è possibile indicare un punto di mount per loro.

Se nel vostro sistema esista già una configurazione LVM valida, essa verrà automaticamente attivata all'inizio della configurazione dell' LVM. Dopo l'attivazione, il partizionamento dei dischi contenenti una partizione che

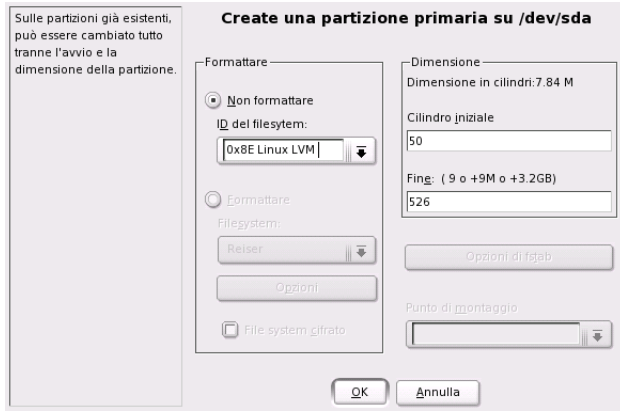

Figura 1.7: *YaST: creare una partizione LVM*

appartenga ad un volume group attivato non potrà essere più modificato. Il kernel di Linux si rifiuterà di leggere un partizionamento modificato, fintanto che anche una sola partizione del rispettivo disco rigido si trovi in uso.

Naturalmente, modificare le partizioni non appartenenti ad un LVM Volume Group non crea problemi. Se nel vostro sistema avete già una configurazione LVM valida, non dovreste avere bisogno di modificare le partizioni. In questa maschera, dovete ora configurare tutti i punti di mount che non si trovano su volumi logici dell' LVM. Almeno il file system root deve trovarsi su una partizione normale. In YaST, selezionate la partizione dalla lista ed impostatela quale file system root facendo clic sul pulsante 'Modifica'.

Dato l'elevato grado di flessibilità dell' LVM, consigliamo di impostare tutti gli altri file system su volumi logici LVM. Dopo aver configurato la partizione di root, potete uscire da questo dialogo.

LVM – creazione dei Physical Volume

In questo dialogo, vengono amministrati i volume group di LVM (spesso abbreviati con "VG"). Se non esiste ancora alcun volume group sul vostro sistema, una finestra pop-up vi inviterà a crearne uno. Come nome da dare al volume group su cui si trovino i file del sistema SUSE LINUX viene proposto `system`.

La cosiddetta Physical Extent Size (abbreviato: PE-size) determina l'estensione massima di un volume fisico e logico all'interno di questo volume

group. Tale valore verrà normalmente fissato su 4 megabyte, consentendo un'estensione massima di 256 gigabyte per un volume fisico e logico. Aumentate questo valore (p.es. a 8, 16 o 32 megabyte) soltanto se avete bisogno di logical volume più grandi di 256 megabyte.

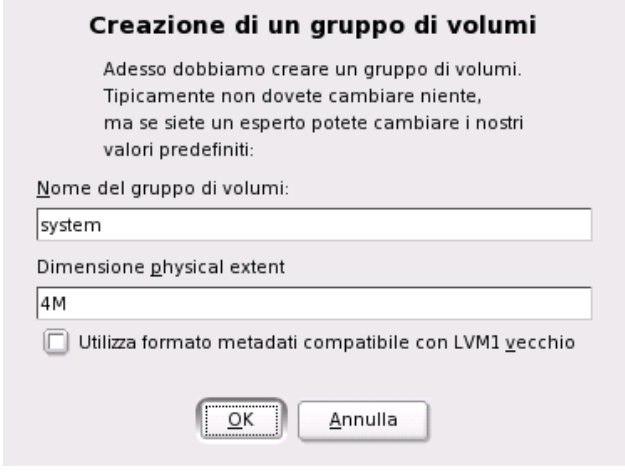

Figura 1.8: *YaST: creare un volume group*

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

Il volume group 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 volume group e cancellarne dei vecchi. Tuttavia, sarà possibile eliminare solo volume group ai quali non è più attribuita alcuna partizione. Per un comune sistema SUSE LINUX installato, non è necessario creare più di un volume group. Una partizione assegnata ad un volume group viene anche definita Physical Volume (spesso abbreviata con: PV).

Per aggiungere una partizione ancora non allocata al volume group selezionato, selezionate la partizione ed attivate la voce 'Aggiungi volume' che si trova sotto la finestra delle selezioni. A questo punto, il nome del volume group verrà riportato nella partizione selezionata. Vi consigliamo di assegnare tutte le partizioni di un LVM ad un volume group, se non volete

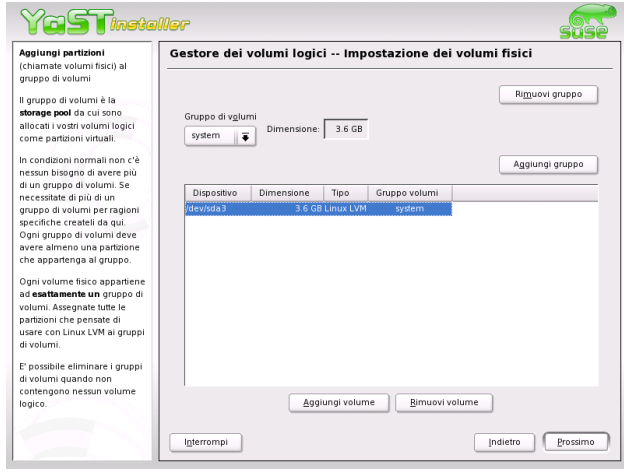

Figura 1.9: *YaST: lista delle partizioni*

lasciare inutilizzato una parte dello spazio della partizione. Prima di chiudere il dialogo, ad ogni volume group dovrà essere attribuito almeno un physical volume.

I Logical Volume

In questo dialogo si amministrano i logical volume (o semplicemente: "LV").

I logical volume vengono assegnati rispettivamente ad un volume group ed hanno un determinata dimensione. Se volete creare un cosiddetto striping array quando create un Logical Volume, dovreste creare innazittutto l' LV con il maggior numero di stripe. 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 Physical Volume. Se chiaramente vi sono solo due PV, non è possibile avere un LV con 3 stripe.

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

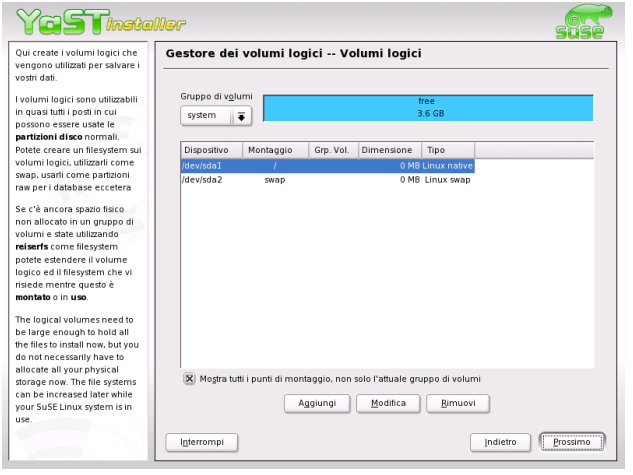

Figura 1.10: *YaST: amministrazione dei Logical Volume*

Attenzione

L'utilizzo del LVM comporta eventualmente una serie dei rischi, come la perdita di dati oppure che dei programmi crollino, vi sia una temporanea caduta di corrente o si immettano dei comandi errati. Salvate i vostri dati prima di utilizzare LVM oppure di riconfigurare i Volume – non lavorate mai senza fare prima una copia di sicurezza!

Attenzione

In caso abbiate configurato già in precedenza un LVM nel vostro sistema, i logical volume esistenti saranno riportati qui. Vi resta, tuttavia, da attribuire a questi logical volume 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 logical volume: 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 creato più di un volume group, potrete passare dall'uno all'altro, servendovi della finestra delle selezione in alto a sinistra. I logical volume esistenti si trovano nel volume group che verrà di volta in volta indicato in alto a sinistra. Disponete i logical volume in ordine di importanza e avrete terminato la configurazione dell'LVM. Potrete ora chiudere il dialogo e

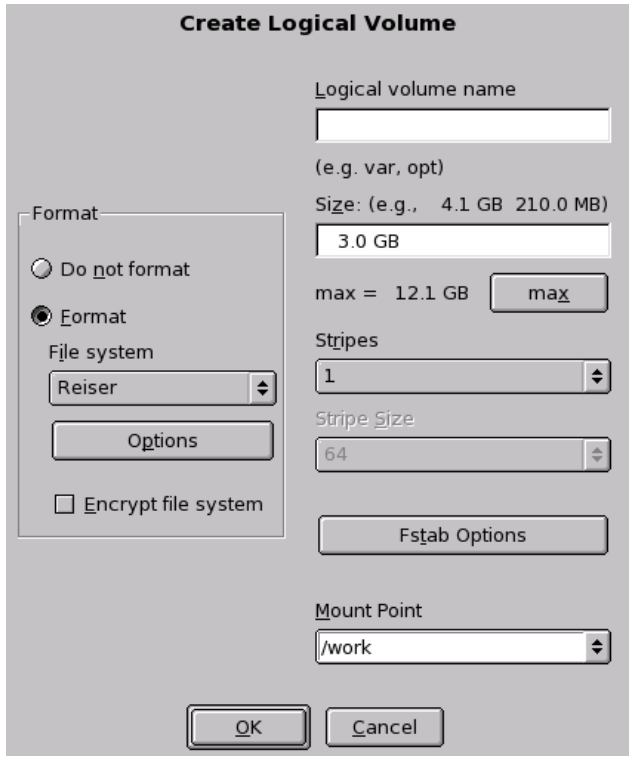

Figura 1.11: *YaST: creare logical volume*

passare alla selezione del software, nel caso in cui vi troviate nel mezzo del processo di installazione

1.9 Soft-RAID

RAID (ingl. *Redundant Array of Inexpensive Disks*) serve ad unificare 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. Il cosiddetto "RAID-Level" definisce il raggruppamento e l'indirizzamento dei dischi rigidi che viene realizzato da un controllore RAID.

Un controllore RAID utilizza normalmente il protocollo SCSI, dal momento che questo gli permette di indirizzare più dischi rigidi in modo migliore di quanto non glielo permetta un protocollo IDE, ed inoltre è più adatto all' elaborazione parallela dei comandi.

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.

1.9.1 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 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 definito *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 %), la prestazione in termini di scrittura risente 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.

RAID 5 RAID 5 rappresenta un compromesso ottimizzato tra i due livelli precedenti, per quel che riguarda prestazione 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 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, bisogna assolutamente impedire che vi sia più di un disco danneggiato alla volta: se

uno viene distrutto, deve essere immediatamente sostituito, affinché non vadano persi dei dati.

1.9.2 Configurazione di Soft-RAID con YaST

Per la configurazione di Soft-RAID dovete ricorrere o ad un apposito modulo 'RAID' sotto 'Sistema', oppure passare per il modulo di partizionamento sotto 'Hardware'.

1. **Passo: partizionare** Per prima cosa, alla voce 'Impostazioni per esperti', nel tool di partizionamento, vedrete un elenco delle vostre partizioni. Se avete già creato delle partizioni Soft-RAID, vi verranno ivi riportate. In caso contrario, dovrete crearne delle nuove. Con RAID 0 e RAID 1, avrete bisogno di almeno due partizioni: di solito con RAID 1 esattamente di due. Se usate invece RAID 5, necessiterete di 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 dei dati dovuto a difetti di un disco nel caso di RAID 1 e 5, nonché per migliorare la prestazione nel caso di RAID 0.

2. **Passo: creazione di RAID** Cliccando su 'RAID', compare il dialogo in cui potrete scegliere tra i livelli RAID 0, 1 o 5. Nella prossima maschera avrete la possibilità di attribuire le partizioni al nuovo RAID. Alla voce 'Opzioni esperti', troverete diverse possibilità di impostazione della "chunk-size": è qui che potrete cesellare la prestazione desiderata. Attivando la casella 'Persistent superblock', le partizioni RAID verranno riconosciute già al primo boot.

   Al termine della configurazione, nella pagina per esperti del modulo di partizionamento, vedrete il dispositivo `/dev/md0` (ecc.) essere contrassegnato come *RAID*.

Troubleshooting Se una partizione RAID è corrotta, ve lo indica il contenuto del file `/proc/mdstats`. In linea di principio, 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 `raidhotadd /dev/mdX /dev/sdX`. Con questo comando, il nuovo disco viene automaticamente integrato nel sistema RAID e altrettanto automaticamente ricostruito.

Per una guida alla configurazione di Soft-RAID ed altri dettagli, consultate l'Howto riportato:

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

o la mailing list di Linux RAID p.es. sotto:

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

Questi indirizzi vi aiuteranno anche nel caso in cui dovessero presentarsi inaspettate difficoltà di una certa complessità.

Aggiornare il sistema e amministrare i pacchetti

SUSE LINUX vi offre la possibilità di aggiornare un sistema, senza doverlo reinstallare. È 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.

2.1 Aggiornare SUSE LINUX

È un fenomeno noto: il software cresce di versione in versione! È 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 vi possa aiutare a decidere di quanto spazio abbiate bisogno: tutto dipende dal tipo di partizione esistente, dal software selezionato e dalla versione da aggiornare a SUSE LINUX.

Nota

È bene leggere il file *README* che trovate sul CD 1 e rispettivamente sotto DOS/Windows, il file, `README.DOS`, dove annotiamo eventuali modifiche effettuate *dopo* che il manuale sia stato dato alla stampa!

Nota

2.1.1 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/lib`. Inoltre è sempre bene scrivere sull'unità di backup anche i dati attuali 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 di root; con il comando `df /` scoprite il nome del dispositivo della vostra partizione root; nel caso dell'output 2.1 è `/dev/hda7` la partizione root da annotare.

Exempio 2.1: *Panoramica con df -h*

```
Filesystem Size Used Avail Use% Mounted on
/dev/hda1  1.9G 189M 1.7G  10%  /dos
/dev/hda2  3.0G 1.1G 1.7G  38%  /
/dev/hda5  15M  2.4M  12M  17%  /boot
```

L'output mostra che la partizione `/dev/hda2` è (montata) nel file system sotto `/`.

Problemi possibili

PostgreSQL Per un update di PostgreSQL (`postgres`), vi consigliamo di fare un dump delle banche dati; cfr. "pg_dump". Ne avrete naturalmente bisogno solo se avete effettivamente usato PostgreSQL prima di aggiornarlo.

I controller della Promise I controller di disco rigido della ditta Promise si trovano su schede madre di qualità di diversi elaboratori, a volte sotto forma di Controller IDE (per UDMA 100) e a volte come controller IDE-RAID. Da SUSE LINUX 8.0 in poi, questi controller vengono supportati direttamente dal kernel come normali controller per dischi rigidi IDE. Solo con il modulo del kernel `pdcraid` viene attivata anche la funzionalità RAID.

A volte accade che dei dischi rigidi con un controller Promise vengano rilevati durante l'update prima di quelli con un normale controller IDE. Il sistema dopo un aggiornamento del kernel non si avvia più ed al boot vi lascia con la frase `Kernel panic: VFS: unable to mount root fs`. In questo caso, durante il boot, dovrete inserire il parametro del kernel `ide=reverse`, per invertire la sequenza di rilevamento dei dischi; cfr. sezione 1.1.2 a pagina 8. Questo parametro dovrà anche essere inserito nella configurazione di boot, con YaST, se avete intenzione di usarlo in modo permanente; cfr. il capitolo *Installazione personalizzata, il boot (Installazione del boot loader)* nel manuale [1].

Attenzione

Vengono rilevati solo i controller abilitati nel BIOS. Attivare o disattivare dei controller si ripercuote sui nomi dei dispositivi. Un errore di configurazione potrebbe rendere impossibile l' eseguire il boot del sistema!

Attenzione

Indicazioni tecniche: la sequenza dei controller dipende dalla scheda madre: ogni casa ha la sua strategia di connessione dei controller supplementari. Con il comando `lspci`, visualizzate questa sequenza. Se il controller Promise viene rilevato prima di quello IDE, è necessario reimpostare il parametro del kernel `ide=reverse` dopo ogni update. Con il vecchio kernel (senza supporto diretto per dispositivi Promise), il controller veniva ignorato ed il normale controller IDE veniva rilevato come primo. Il primo disco era `/dev/hda`. Con il nuovo kernel, il controller Promise viene rilevato direttamente ed i suoi (fino a quattro) dischi sono `/dev/hda`, `/dev/hdb`, `/dev/hdc`

e `/dev/hdd`. Quello che finora era `/dev/hda` diventa `/dev/hde` e quindi non viene più rilevato durante il boot.

2.1.2 L'update con YaST

Dopo i preparativi riportati nella sezione 2.1.1 a pagina 44 avviate il sistema.

1. Avviate il sistema come per un'installazione (cfr. manuale dell'utente) e, 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; se no continua con la backup del sistema. Se vi sono più partizioni, selezionate la partizione giusta e confermate la vostra selezione con 'Prossimo' (nell'esempio nella sezione 2.1.1 a pagina 44 avevate annotato `/dev/hda7`).

   YaST leggerà il vecchio `fstab` che si trova su questa partizione, per analizzare ed eseguire il mount dei 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 una 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.

2.1.3 L'update manuale

Aggiornare il sistema di base

Poiché, all'aggiornamento del sistema di base devono venire modificate anche le parti centrali del sistema (p.es. le librerie), questo compito non può essere svolto mentre il sistema è in esecuzione.

Dovrete quindi inizializzare l'ambiente di aggiornamento. Normalmente, si usa il CD o DVD, oppure il dischetto di caricamento che avete creato in precedenza (bootdisk). Se desiderate intervenire manualmente sull'aggiornamento o di eseguirlo del tutto con ncurses-ui di YaST (modo di testo), seguirete più o meno la procedura descritta nella sezione 1.1 a pagina 8 ss.:

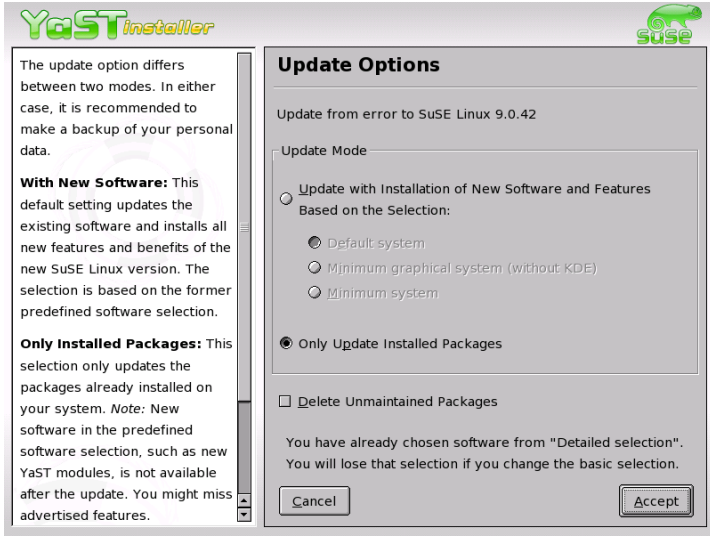

Figura 2.1: *Update del software*

1. Subito dopo il boot del kernel dal bootdisk o dal CD o DVD viene lanciato automaticamente linuxrc.
2. Con linuxrc, dovrete innanzitutto stabilire la lingua e mappatura della tastiera nel menù principale, alla voce 'Impostazioni'. Confermate con 'Ok'.
3. Tramite la voce di menu 'Moduli kernel' eventualmente vanno caricati i driver di software ed hardware richiesti; per maggiori dettagli sulla procedura da seguire, rimandiamo alla sezione 1.1.3 a pagina 10 e la descrizione di linuxrc 12.4.4 a pagina 280.
4. Una volta fatto ciò, si può passare, tramite le voci di menu 'Avvia installazione / sistema' -> e 'Inizializza installazione/update', alla scelta del supporto di installazione. (vedi 12.4.6 a pagina 281).
5. Dopodiché, linuxrc inizializza l'ambiente di installazione e viene lanciato YaST.

Nel menù iniziale di YaST – dopo che YaST abbia controllato le impostazioni della lingua e dell'hardware – scegliete la voce 'Aggiorna sistema esistente'.

In seguito, YaST cerca la partizione root e mostra il risultato. Selezionate o confermate una delle partizioni: indicate nell'elenco la vostra partizione root che avete annotato prima (nell'esempio: `/dev/hda2`). In questo modo. istruite YaST a leggere il vecchio `fstab` che si trova su questa partizione. YaST analizzerà ed in seguito monterà i file system lì registrati.

Avrete poi la possibilità di creare una copia di sicurezza dei file di sistema durante l'aggiornamento.

Nel dialogo successivo, potrete decidere se aggiornare solo il software già installato o aggiungere al sistema nuovi componenti di software (modo upgrade). Vi consigliamo di accettare quanto vi viene proposto (ad esempio 'Sistema standard'). Con YaST potrete ovviare ad eventuali incongruenze.

Dialogo di avvertimento: 'Sì', per rendere possibile il trasferimento del nuovo software dal supporto sorgente al disco rigido del sistema. Segue la verifica della banca dati RPM.

Infine, verranno attualizzate le parti centrali del sistema, laddove YaST approntera automaticamente delle copie di sicurezza di tutti quei file che sono stati modificati dall'ultima installazione. Poi, vengono archiviate vecchie versioni dei file di configurazione (che di solito hanno l'estensione `.rpmorig` o `.rpmsave`; il processo di installazione o update viene protocollato in `/var/adm/inst-log/installation-*` e potrà essere consultato in qualsiasi momento.

Update del resto del sistema

Una volta aggiornato il sistema di base, accedete ad uno speciale modo di update di YaST. Lì, potete aggiornare il resto del sistema in base alle vostre preferenze.

Una volta eseguito questo compito, dovete terminare il processo come se si trattasse di una normale installazione: fra l'altro, dovreste scegliere un nuovo kernel; YaST vi offrirà questa opzione.

Nota

Se fate il boot con loadlin, dovrete copiare il kernel *nuovo* e eventualmente il file `initrd` nella directory `loadlin` della vostra partizione DOS!

Nota

Problemi possibili

Se, dopo l'update, alcuni ambienti shell non reagiscono come di consueto, verificate immediatamente se i cosiddetti file punto attuali nella home directory siano ancora compatibili con il sistema. In caso contrario, caricate le versioni attuali da `/etc/skel`; esempio: `cp /etc/skel/.profile /.profile`.

2.1.4 Aggiornare singoli pacchetti

Oltre all'update completo, potete naturalmente aggiornare anche i singoli pacchetti; per farlo, dovete naturalmente fare *voi stessi* attenzione che il sistema rimanga consistente: al momento potete trovare dei consigli all'URL: `http://www.suse.de/en/support/download/updates/`

Nella scelta dei pacchetti tramite YaST potete fare quello che volete. Se scegliete di aggiornare un pacchetto importante per il funzionamento del sistema, YaST vi avviserà: tali pacchetti dovrebbero venire aggiornati nel modo speciale di update. Molti pacchetti contengono per esempio shared libraries, che vengono probabilmente utilizzate dai processi in corso al momento dell'aggiornamento stesso. Un aggiornamento con il sistema in esecuzione potrebbe portare al malfunzionamento di questi programmi.

2.2 Da versione a versione

Nelle sezioni successive elenchiamo quali dettagli sono cambiati da una versione all'altra. In questo sommario vedete per esempio se sono state modificate delle impostazioni fondamentali o se sono stati spostati dei file di configurazione o se sono stati modificati dei noti programmi. Attireremo la vostra attenzione solo su quelle cose rilevanti per il lavoro quotidiano dal punto di vista dell'utente o dell'amministratore di sistema. L'elenco non è completo.

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.suse.de/en/support/download/updates/`.

2.2.1 Dalla versione 7.3 alla 8.0

Problemi e particolarità: `http://sdb.suse.de/sdb/en/html/bugs80.html`.

- I dischetti di caricamento sono disponibili solo sotto forma di immagini di dischetto (finora la directory `disks`, adesso `boot`). Avrete bisogno di un dischetto di caricamento solo se non riuscirete a caricare il sistema dal CD; inoltre, a seconda dell'hardware o modalità di installazione vanno creati altri dischetti dalle cosiddette image `modules1`, `modules2` etc.; per sapere come procedere, cfr. 1.4 a pagina 18 o 1.4.2 a pagina 20.
- YaST2 ha ormai completamente soppiantato YaST1, anche nel modo di testo/console. Quando parleremo di YaST si intende la nuova versione.
- Alcuni BIOS hanno bisogno del parametro del kernel `realmode-power-off`; fino alla versione del kernel 2.4.12, questo parametro si chiamava `real-mode-poweroff`.
- Le variabili `START` di `rc.config`, usate per avviare i servizi, non sono più necessarie. Tutti i servizi vengono avviati se i relativi link sono presenti nelle rispettive directory dei runlevel; per creare i link, immettete il comando `insserv`.
- I servizi di sistema vengono configurati tramite i valori delle variabili nei file in `/etc/sysconfig`; quando eseguite un aggiornamento, vengono automaticamente adottati i file in `/etc/rc.config.d`.
- `/etc/init.d/boot` è stato suddiviso in diversi script e, dove sensato, spostato in altri pacchetti (cfr. `kbd`, `isapnp`, `lvm` etc.) ; cfr. 13.4 a pagina 297.
- Nell'ambito della rete sono stati introdotti serie di cambiamenti; cfr. la sezione 14.4 a pagina 335.
- Per amministrare i file di protocollo *log file*, si usa il programma logrotate; `/etc/logfiles` non è più necessario ; cfr. la sezione 12.2.3 a pagina 268.
- Il login di `root` tramite telnet o rlogin può essere impostato nei file sotto `/etc/pam.d`; non è tuttavia più possibile impostare `ROOT_LOGIN_REMOTE` su `yes`, per motivi di sicurezza.
- `PASSWD_USE_CRACKLIB` può essere attivato con YaST.
- Se desiderate distribuire i file NIS per `autofs` tramite NIS, usate il modulo client NIS di YaST per la configurazione; attivate 'Avviare automounter'. La variabile `USE_NIS_FOR_AUTOFS` non è quindi più necessaria.

- locate, usato per trovare subito dei file, non appartiene più al software che viene installato di default. Se necessario, installatelo in un secondo momento (`find-locate`) e vedrete che, circa un quarto d'ora dopo aver acceso il computer, verrà automaticamente avviato il processo updatedb!
- Per pine è abilitato il supporto del mouse. Questo vuol dire che potete cliccare sulle voci di menu con il mouse quando utilizzate Pine in un xterm (o simili). Inoltre dovete considerare che il cut & paste, cioè taglia & incolla funziona solo con il tasto Shift premuto, sempre se il supporto per il mouse è abilitato. Quando eseguite una nuova installazione tale supporto è disabilitato. Se eseguite un aggiornamento non è da escludere che questa funzione sia abilitata (se vi è un `~/.pinerc` non più recente). In questo caso potete disabilitare nella configurazione di Pine l'opzione `enable-mouse-in-xterm`.

2.2.2 Dalla versione 8.0 alla 8.1

Problemi e particolarità: `http://sdb.suse.de/sdb/en/html/bugs81.html`.

- Modificare i nomi degli utenti e dei gruppi del sistema: per essere consistenti con United Linux, sono state adattate alcune registrazioni in `/etc/passwd` o `/etc/group`.
  - Utenti modificati: `ftp` ora si trova nel gruppo `ftp` (non più in `daemon`).
  - Gruppi rinominati: `www` (ex `wwwadmin`); `games` (ex `game`).
  - Nuovi gruppi: `ftp` (con GID `50`); `floppy` (con GID `19`); `cdrom` (con GID `20`); `console` (con GID `21`); `utmp` (con GID `22`).
- Le modifiche relative all' FHS (cfr. sezione 12.1.2 a pagina 266):
  - Un'ambiente esempio per HTTPD (Apache) si genera sotto `/srv/www` (ex `/usr/local/httpd`).
  - Un'ambiente esempio per FTP si genera sotto `/srv/ftp` (ex `/usr/local/ftp`). É richiesto il pacchetto `ftpdir`.
- Per consentire un accesso mirato al software che cercate, alcuni pacchetti non risiedono più in serie difficile da identificare, ma in chiari gruppi RPM. La conseguenza è che non esistono più directory enigmatiche sotto `suse` sui CD, ma solo poche directory che portano il nome dell'architettura come p.es. `ppc`, `i586` o `noarch`.

- Se eseguite una nuova installazione, ecco cosa cambia:
  - viene installato il bootloader GRUB che offre decisamente più possibilità di LILO. Comunque, rimane la possibilità di continuare ad usare LILO dopo aver eseguito un *aggiornamento* del sistema.
  - il mailer postfix prende il posto di sendmail.
  - al posto di majordomo viene installato il software moderno per mailing list mailman.
  - harden_suse è da selezionare manualmente e leggete la documentazione!
- Pacchetti suddivisi: `rpm` in `rpm` e `rpm-devel`; `popt` in `popt` e `popt-devel`; `libz` in `zlib` e `zlib-devel`.

  `yast2-trans-*` è adesso suddiviso anche secondo le lingue: `yast2-trans-cs` (ceco), `yast2-trans-de` (tedesco), `yast2-trans-es` (spagnolo) etc.; durante l'installazione non vengono più installate tutte le lingue per risparmiare dello spazio sul disco. All'occorrenza potete installare in un secondo momento i pacchetti necessari per il supporto della vostra lingua di YaST.
- Pacchetti che cambiano nome: `bzip` diventa `bzip2`.
- Pacchetti non più inclusi: `openldap`, utilizzate adesso `openldap2` e `sudo` al posto di `su1`.

2.2.3 Dalla versione 8.1 alla 8.2

Problemi e particolarità: `http://sdb.suse.de/sdb/en/html/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; cfr. 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 ora il motore DSSSL che 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, dovrete adattare le applicazioni in base a `/usr/share/sgml/openjade` oppure creare un link come `root`:

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

  Per evitare un conflitto con l'applicazione rzsz, il tool per la riga di comando `sx` continua a chiamarsi `s2x`/`sgml2xml` oppure `osx`.

2.2.4 Dalla versione 8.2 alla 9.0

Problemi e particolarità: `http://sdb.suse.de/sdb/en/html/bugs90.html`

- I servizi di manutenzione ad intervalli regolari in `/etc/cron.daily`, `/etc/cron.weekly` e `/etc/cron.monthly` vengono eseguiti alle 4:00, questa indicazione temporale vale solo se si esegue una nuova installazione; dopo un update va adattato eventualmente `/etc/crontab` .

- É disponibile adesso la versione 4 del programma di gestione di pacchetti RPM. La funzione per compilare i pacchetti si trova adesso nel programma a sé stante `rpmbuild`; potete continuare a utilizzare `rpm` per l'installazione, l'aggiornamento e l'interrogazione della banca dati; cfr. la sezione 2.3 a pagina 57.
- Per quel che riguarda il processo di *stampa* vi è il pacchetto `footmatic-filters`. Il contenuto è stato preso dal `cups-drivers`, visto che con esso è possibile 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 resi 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.

2.2.5 Dalla versione 9.0 alla 9.1

Problemi e particolarità: `http://sdb.suse.de/sdb/en/html/bugs91.html`.

- 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.

- Per quel che riguarda i dispositivi di immissione (*Input devices*) cfr. l'articolo riportato sopra.
- 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*). Da un punto di vista del porting è da preferire NPTL dato che si tratta dello standard di prossima generazione.

  In caso di difficoltà con NPTL si può ripiegare su implementazioni antecenti di linuxthreads impostando le seguenti variabili di ambiente (⟨*versione_del_kernel*⟩ va sostituito con il numero di versione del rispettivo kernel):

  ```
  LD_ASSUME_KERNEL=versione_del_kernel
  ```

  Ecco i numeri di versione possibili:

  2.2.5 (i386, s390): linuxthreads senza floating stack

  2.4.1 (AMD64, IPF, s390x, 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`. Programmi C++ con supporto multithread che utilizzano *Thread Cancellation*, vanno impostati in modo che utilizzano la libreria linuxthreads impostando la variabile di ambiente `LD_ASSUME_KERNEL=2.4.1` .
- NPTL (*Native POSIX Thread Library*) è incluso come pacchetto thread in SUSE LINUX 9.1. NPTL è stato sviluppato in modo binariamente compatibile (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; `getpid` ritorna in tutti i thread lo stesso valore; thread handler, registrati con pthread_atfork non funzionano se si utilizza `vfork`.

- Di default si ha la codifica `UTF-8`. Durante l'installazione standard, si avrà un "locale" con `.UTF-8` quale codifica (*Encoding*) (p.es. `it_IT.UTF-8`).
- 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 ed è il valore di default per `_POSIX2_VERSION`. E' possibile consultare lo standard SUS (liberamente, ma è richiesta la registrazione):

  `http://www.unix.org`

  Ecco un breve confronto:

  Tabella 2.1: *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 +3
nice -10	nice -n 10
split -10	split -l 10

Nota

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`.

Nota

- `/etc/gshadow` è stato rimosso, essendo diventato superfluo; ecco i motivi:
  - ▷ la glibc non lo supporto.

- 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 ed lo ignorano per le ragioni appena menzionate.

- FHS (si veda 12.1.2 a pagina 266) prevede che risorse XML (DTD, stylesheet etc.) vengano installati 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`.

2.3 RPM – Il package-manager della distribuzione

SUSE LINUX ricorre a RPM (`rpm`) *RPM Package Manager*, con i programmi principali `rpm` e `rpmbuild`, per amministrare i pacchetti software. 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*, cioè non modificati, allo stato originale.

Gli archivi RPM installabili vengono compressi in uno speciale formato binario; gli archivi sono composti di file da installare e di 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 12.1.1 a pagina 266.

Nota

In alcuni pacchetti, i componenti necessari allo sviluppo di software (biblioteche, file header ed include, ecc.) sono stati raccolti in pacchetti a se stanti. Questi pacchetti sono necessari soltanto quando si intende compilare *da soli* del software (ad esempio, nuovi pacchetti GNOME). Generalmente, essi sono riconoscibili dall'estensione `-devel`: `alsa-devel`, `gimp-devel`, `kdelibs-devel` etc.

Nota

2.3.1 Controllare l'autenticità di un pacchetto

I pacchetti RPM di SUSE vengono firmati con GnuPG:

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

Con il comando `rpm --checksig apache-1.3.12.rpm` si può controllare la firma di un pacchetto RPM e in questo modo stabilire se proviene veramente da SUSE; cosa consigliabile specialmente quando si scaricano pacchetti di aggiormanento dall'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 che anche l'utente normale possa controllare la firma dei pacchetti RPM.

2.3.2 Amministrare i pacchetti: installarli, aggiornarli e disinstallarli

Normalmente, installare un archivio RPM è una questione di pochi attimi: `rpm -i` ⟨*`pacchetto.rpm`*⟩. Con questo comando standard, 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, è possibile aggirare questa regola – chi lo fa deve sapere perfettamente ciò che sta facendo, poiché ciò può mettere 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>
```

In questo modo viene cancellata una versione vecchia del pacchetto ed installata quella nuova. La differenza tra le due versioni è che con `-U` vengono installati anche pacchetti che finora non sono disponibili nell sistema, mentre con l'opzione `-F` un pacchetto viene aggiornato solo se installato in precedenza. Contemporaneamente `rpm` cerca di intervenire con cautela sui *file di configurazione* applicando – detto in maniera un pò semplificata –la seguente strategia:

- Se un file di configurazione *non* è stato modificato dall'amministratore di sistema, `rpm` installa la nuova versione del file relativo. Un intervento da parte dell'amministratore non è più necessario.
- Se un file di configurazione è stato modificato prima dell'aggiornamento, `rpm` memorizzerà con l'estensione `.rpmorig` o `.rpmsave` 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 d'aggiornamento. In questo caso è molto probabile che dobbiate adattare il file di configurazione appena installato in base alla copia di sicurezza (`.rpmorig` o `.rpmsave`).
- I file `.rpmnew` appaiono se il file di configurazione esiste già *e* se nel file `.spec` è stato attivato `noreplace`.

Alla fine di un update, dopo l'adattamento, si devono rimuovere tutti i file `.rpmorig`-, `.rpmsave`- o `.rpmnew` per non essere d'impaccio ai futuri update. L'estensione `.rpmorig` viene scelta se il file era sconosciuto alla banca dati RPM, altrimenti si ha l'estensione `.rpmsave`. Cioè: `.rpmorig` si ha quando si fa 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 eseguito una modifica nel 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 si possa continuare a lavora senza interruzione con le proprie impostazioni.

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

Nota

Dopo ogni aggiornamento dovete controllare le copie di sicurezza con l'estensione `.rpmorig` o `.rpmsave` create da `rpm`; si tratta dei vostri vecchi file di configurazione. Se necessario, assumete i vostri adattamenti dalle copie di sicurezza ed inseritele nei nuovi file di configurazione, e cancellate quindi i vecchi file con l'estensione `.rpmorig` o `.rpmsave`.

Nota

Procedura per cancellare un pacchetto: `rpm -e` ⟨*pacchetto*⟩.

`rpm` elimina un pacchetto solo quando non esistono più delle dipendenze;. p.es. è teoreticamente impossibile cancellare Tcl/Tk finchè richiesto da un programma – anche qui fa la guardia RPM con il suo database. Se, in casi eccezionali, non è possibile cancellare un pacchetto, benchè non ci sia alcuna dipendenza, può essere d'aiuto creare di nuovo il database RPM con l'aiuto dell'opzione `--rebuilddb`; si vedano più avanti le note sull'RPM database (sezione **??** a pagina ??).

2.3.3 RPM e patch

Per garantire la sicurezza di un sistema è 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. A partire dalla versione 8.1 SUSE offre una nuova feature di RPM che consente di installare delle patch per pacchetti.

Vogliamo illustrare le caratteristiche di maggior interesse di una RPM patch prendendo pine come esempio:

- La RPM patch va bene per il mio sistema?

  Per poter rispondere a questa domanda bisogna sapere quale versione del pacchetto è installata. Nel caso di pine immettete il comando `rpm -q pine pine-4.44-188`.

  Ora viene analizzato se l'RPM patch va bene per questa versione di pine:

```
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 le tre versioni di pine riportate. Visto che è inclusa anche la nostra, possiamo installare la patch.

- Quali file vengono sostituiti dalla patch?

  I file interessati possono essere letti facilmente da una RPM patch. Il parametro `-P` di rpm serve a selezionare determinate feature della patch, e con

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

  si ottiene un elenco dei file, o se la patch è già installata l'elenco si ottiene con

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

- Come si installa una RPM patch?

  Alla stregua di RPM 'normali'. L'unica differenza è che deve essere già installato un RPM adatto alla RPM patch.

- Quali patch sono installate nel sistema e su quale versione del pacchetto si basano?

  Un elenco delle patch installate si ottiene con il comando `rpm -qPa`. Se, come nel nostro esempio, in un sistema nuovo è stata installata finora solo una patch, si avrà: `rpm -qPa pine-4.44-224`.

  Se dopo un certo periodo di tempo volete sapere quale versione del pacchetto è stata installata originariamente, consultate la banca dati di RPM. Nel caso di `pine` immettete il comando `rpm -q --basedon pine pine = 4.44-188`.

Ulteriori informazioni, anche sulle feature della patch di RPM, sono reperibili nella `man rpm` oppure nella `man rpmbuild`.

2.3.4 Inoltrare richieste

Con l'opzione `-q` *query* si crea una richiesta. Con essa è possibile sia rovistare negli archivi RPM (opzione `-p pacchetto_file`) che interrogare la banca dati RPM. Le modalità di risposta possono venire impostate tramite ulteriori parametri; cfr la tabella 2.2.

Tabella 2.2: *Le opzioni di richiesta più importanti (-q [-p] … pacchetto)*

`-i`	mostra le informazioni sul pacchetto
`-l`	mostra la lista dettagliata dei file
`-f FILE`	richiesta al pacchetto che contiene il file `FILE`; `FILE` deve venire indicato con il percorso completo!
`-s`	mostra lo stato del file (implica `-l`)
`-d`	elenca solo i file di documentazione (implica `-l`)
`-c`	elenca solo i file di configurazione (implica `-l`)
`--dump`	mostra tutte le informazioni verificabili di ogni file (usare insieme a `-l`, `-c` o `-d`!)
`--provides`	elenca le funzionalità del pacchetto che possono venire richieste da un altro pacchetto con `--requires`
`--requires`, `-R`	elenca le dipendenze del pacchetto
`--scripts`	elenca i diversi script di (dis)installazione

Il comando `rpm -q -i wget` elenca le informazioni nell'output 2.2:

Exempio 2.2: *rpm -q -i wget*

```
Name        : wget                     Relocations: (not relocateable)
Version     : 1.8.2                    Vendor: SuSE Linux AG, Nuernberg, Germany
Release     : 301                      Build Date: Di 23 Sep 2003 20:26:38 CEST
Install date: Mi 08 Okt 2003 11:46:31 CEST      Build Host: levi.suse.de
Group: Productivity/Networking/Web/Utilities Source RPM: wget-1.8.2-301.src.rpm
Size        : 1333235                         License: GPL
Signature   : DSA/SHA1, Di 23 Sep 2003 22:13:12 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` ha l'effetto desiderato se si conosce il nome del file completo, incluso il percorso; si può inserire una quantità qualsiasi di file da cercare, p.e.: `rpm -q -f /bin/rpm /usr/bin/wget` porta al risultato:

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

Se si conosce solo una parte del nome del file ci si deve aiutare con uno shell script (cfr. 2.3); il nome del file cercato è da indicare come parametro alla chiamata dello script.

Exempio 2.3: *Script cerca-pacchetti*

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

Con il comando `rpm -q --changelog rpm` ci si può far mostrare l'elenco le informazioni (update, configurazione, modifiche etc.) su un determinato pacchetto; vediamo 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 è montato su `/cdrom` potete fare le vostre query.

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

In base alla banca dati 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 originale (cioè quella contenuta nel pacchetto). `rpm` antepone al vero e proprio nome di file fino ad otto caratteri, i quali indicano le seguenti modifiche:

Tabella 2.3: *I controlli*

5	somma di controllo MD5
S	grandezza del file

`L` link simbolico

`T` ora della modifica

`D` major e minor *device number*

`U` utente *user*

`G` gruppo *group*

`M` modo (incl. diritti e tipo)

Nei file di configurazione viene emessa anche una `c`. Per esempio, nel caso sia stato modificato qualcosa in `/etc/wgetrc` del `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 GB, la banca dati può senz'altro riservarsi 30 MB di spazio sull' hard disk; specialmente dopo un aggiornamento completo. Se la banca dati sembra essere troppo grande è 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 MB per ogni back-up con una `/usr` di 1 GB.

2.3.5 Installare e compilare i pacchetti dei sorgenti dei pacchetti

Tutti i sorgenti *sources* di SUSE LINUX terminano in `.src.rpm`, si tratta di source-RPM.

Nota

Come ogni altro pacchetto, anche questi possono venire installati tramite YaST; i pacchetti dei sorgenti non vengono però mai contrassegnati come installati (`[i]`), come nel caso invece dei pacchetti normali. Ciò dipende dal fatto che i pacchetti dei sorgenti non vengono registrati nella banca dati RPM; in essa infatti appare solo software *installato*.

Nota

Le directory di lavoro di rpm oppure `rpmbuild` sotto `/usr/src/packages` devono essere presenti (nel caso non si sia fatta una propria configurazione p.e. tramite `/etc/rpmrc`):

SOURCES per i sorgenti originali (file `.tar.gz` etc.) e per gli adattamenti specifici della distribuzione (file `.dif`).

SPECS per i file `.spec`, simili a meta-makefile, che controllano il processo build.

BUILD sotto questa directory, i sorgenti vengono scompattati, "patchati" e compilati.

RPMS qui vengono archiviati i pacchetti binari pronti.

SRPMS e qui i source-RPM.

Se installate con YaST un pacchetto sorgente, 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`.

Nota

Non fate esperimenti con gli RPM e componenti importanti del sistema (`libc`, `rpm`, `nkit`, etc.); altrimenti mettete a repentaglio la funzionalità del vostro sistema.

Nota

Osserviamo ora il pacchetto `wget.src.rpm`. Dopo aver installato il pacchetto sorgente `wget.src.rpm` con YaST vi sono i file:

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

Con `rpm -b X /usr/src/packages/SPECS/wget.spec` viene inizializzato il processo di compilazione; la variabile `X` può stare per diversi gradi (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 patchare.

-bc come `-bp`, con compilazione.

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

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

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

Con l'opzione -short-circuit è possibile saltare singoli passi. L'RPM binario creato alla fine deve venire installato con rpm -i o meglio con rpm -U.

2.3.6 Creare pacchetti RPM con build

Nel caso di molti pacchetti sussiste il pericolo che durante la loro compilazione involontariamente dei file vengono copiati sul 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 dei 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 <percorso>. A differenza di rpm, il comando build preferisce avere il file SPEC nella stessa directory dei sorgenti. Se come nell'esempio riportato sopra volete ricompilare wget e il DVD è 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 dei livelli descritti sopra. Per avere maggiori dettagli digitate il comando build --help e consultate la pagina di manuale man build.

2.3.7 Tool per gli archivi RPM e la banca dati RPM

Il Midnight Commander (`mc`) è, di per sé, in grado di mostrare il contenuto di un archivio RPM e di copiarne delle parti. L'archivio viene raffigurato come file system virtuale, di modo che siano disponibili i punti nel menu di Midnight Commander: le informazioni dell'header del file `HEADER` possono venire visualizzate premendo (F3); con i tasti-cursore e con (Enter) è possibile navigare nell'archivio, e all'occorrenza copiarne delle componenti con (F5). A proposito, anche per Emacs esiste un `rpm.el`, un front-end per rpm.

KDE contiene il tool kpackage. GNOME vi offre gnorpm.

Con Alien (`alien`) è possibile convertire i formati dei pacchetti delle diverse distribuzioni. In questo modo si può tentare, *prima* dall'installazione, di convertire vecchi archivi TGZ in RPM, affinchè, *durante* l'installazione stessa, la banca dati RPM venga rifornita con le informazioni dei pacchetti. Ma ATTENZIONE: `alien` è uno script Perl, e come informano gli autori, si trova ancora in fase "alpha" – nonostante abbia già raggiunto un numero di versione abbastanza elevato.

Parte II

Configurazione

YaST nel modo testo (ncurses)

Questo capitolo 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 questo capitolo verrà trattato l'uso di YaST nel modo testo (ncurses). Inoltre indicheremo come aggiornare in linea il sistema per essere sempre al passo coi tempi.

3.1 L'uso

Con i tasti (Tab), (Alt) + (Tab), (barra spaziatrice), tasti freccia ((↑) e (↓)) ed (Enter) nonché gli shortcut si lascia maneggiare in fin dei conti l'intero programma.

3.1.1 Il centro di controllo YaST

Se avviate YaST nel modo testo apparirà come prima cosa la finestra principale (vd. 3.1).

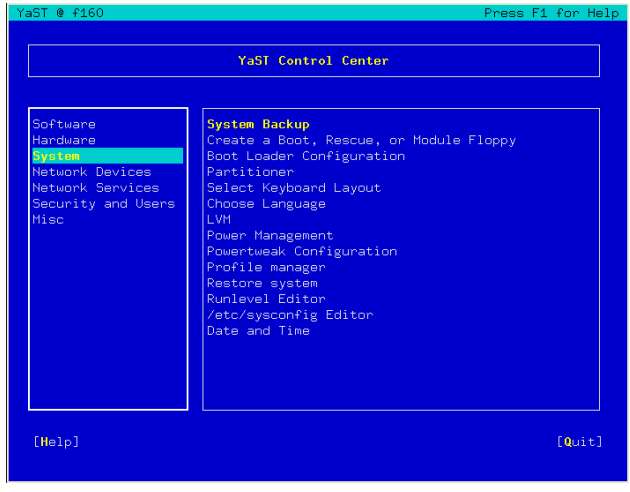

Figura 3.1: *La finestra principale di YaST-ncurses*

Qui avete tre settori: nella colonna a sinistra vedete le categorie in cui sono suddivisi i diversi moduli. La categoria attiva viene evidenziata. A destra avete i moduli della categoria evidenziata. Sotto i due bottoni per richiedere assistenza ed uscire.

Dopo 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 è stato selezionato un modulo, il modulo assume un colore diverso, e sotto vedrete una breve descrizione del modulo.

Con Enter 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 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 Enter.

3.1.2 I moduli YaST

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 mappati. Per le possibili eccezioni vi rimandiamo alla sezione 3.2 nella pagina seguente.

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, p.es. i singoli moduli di un gruppo di moduli nel centro di controllo. Se delle singole voce all'interno di un riquadro dovessero non rientrare in larghezza nel riquadro, spostatevi con Shift–→ o Shift–← orizzontalmente verso destro e sinistra (alternativamente funzione 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, radiobottoni 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 Enter. Alternativamente potete selezionare in modo mirato radiobottoni e checkbox come normali bottoni tramite Alt–lettera_gialla . In questo caso non serve confermare ancora una volta con Enter. Tramite il tasto Tab è necessario un ulteriore Enter, affinché l'azione selezionata venga eseguita o la relativa voce di menu venga abilitata (cfr. la fig. 3.2 nella pagina successiva).

I tasti funzione Anche i tasti da (F1 a F12) sono mappati. Vi permetteranno di indirizzare direttamente dei bottoni. Quale funzione viene eseguita da quale tasto dipende dal modulo nel quale vi trovate in

YaST visto che nei diversi moduli sono disponibili diversi bottoni (p.es. dettagli, informazioni, aggiungi, cancella ...). Per gli amici di YaST1 i bottoni 'OK', 'Prossimo' e 'Fine' vengono eseguiti con il tasto F10. In YaST con il tasto F1 vi potete fare indicare le funzioni dei tasti funzione.

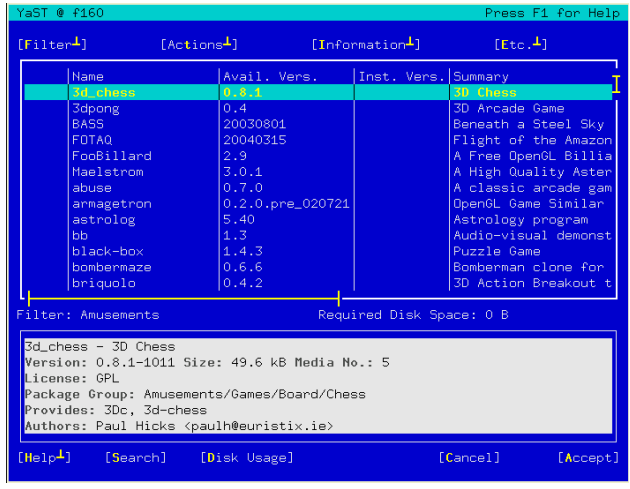

Figura 3.2: *Il modulo per l'installazione del software*

3.2 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 mappati dalle impostazioni del terminale che usate.

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: Anche i tasti funzione sono già occupati. Anche in questo caso determinati tasti funzioni possono essere mappati attraverso la scelta del terminale, e non essere quindi disponibili per YaST. In una console puramente testuale le combinazioni con Alt e i tasti funzione dovrebbero essere comunque tutti disponibili.

3.3 Richiamare singoli moduli

Per risparmiare del tempo, ogni modulo di YaST può essere richiamato singolarmente, basta immettere: `yast nome_del_modulo`.

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`.

3.4 YOU: YaST Online Update

3.4.1 Il modulo YOUI

Potete lanciare YOU anche dalla riga di comando immettendo come `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 delle patch ed informazioni. Se non indicate subito una url, selezionate il server/ la directory tramite la maschera di YaST. La maschera funziona in modo analogo al modulo YaST grafico descritto nel *Manuale dell'utente*. Come per la versione grafica di YaST anche qui potete impostare un job di cron tramite il bottone 'Configura l'aggiornamento in modo automatico'.

3.4.2 Aggiornamento in linea dalla riga di comando

Con il tool da riga di comando online_update potete eseguire un update del vostro sistema ad es. con degli script.

Volete impostare il vostro sistema in modo che ad un orario determinato esegua una ricerca degli update su di un determinato server, scarichi le patch e le relative informazioni senza però installarle, visto che in un secondo momento volete prenderle in visione e selezionare i pacchetti da installare:

- Impostate un job di cron che esegua questo comando:

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

  `-u` introduce la URL di base dell'albero directory da cui prelevare le patch. Vengono supportati i protocolli `http`, `ftp`, `smb`, `nfs`, `cd`, `dvd` e `dir`. Con `-g` scaricate le patch in una directory locale senza installarla, come opzione potete applicare un filtro alle patch in base ai tre tipi `security` (update di sicurezza), `recommended` (update consigliabili) ed `optional` (update opzionali). Se non indicate un filtro online_update scarica tutte le nuove patch disponibili del tipo `security` e `recommended`.

- Una volta scaricati i pacchetti potete installarli immediatamente o prenderli in visione. online_update salva le patch nel percorso `/var/lib/YaST2/you/mnt/`. Con il seguente comando installate le patch:

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

  Il parametro `-u` indica la URL locale dove trovare le patch da installare. `-i` avvia il processo di installazione.

- Se volete analizzare le patch scaricate prima dell'installazione ed eventualmente scartarne alcune, lanciate la maschera YOU:

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

  YOU si avvia e come fonte delle patch ricorre alla directory locale contenenti le patch scaricate in precedenza invece che ad una directory remota su Internet. In seguito selezionate le patch desiderate come per il normale processo di installazione tramite il gestore dei pacchetti.

Per ulteriori informazioni su online_update date una occhiata all'output del comando `online_update -h`.

Il sistema X-window

Sotto Unix il sistema X-window (X11) rappresenta quasi lo standard in tema di GUI (interfaccia grafica dell'utente), e questo non è tutto: X11 è un sistema basato sulla rete; 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, cioè i computer possono anche comunicare via Internet.

In questo capitolo, vi illustreremo come ottimizzare il vostro ambiente del sistema X window, faremo luce alcune nozioni fondamentali riguardanti l'utilizzo di font sotto SUSE LINUX e trattremo la configurazione di OpenGL/3D. La descrizione del modulo YaST per la configurazione dello schermo, scheda grafica, mouse e tastiera è reperibile nel *Manuale dell'utente*.

X11 ebbe origine come prodotto realizzato congiuntamente da DEC™ (Digital Equipment Corporation™) e dal progetto Athena al MIT™ (Massachusetts Institute of Technology™). La prima versione (X11R1) venne rilasciata nel settembre del 1987. Dalla versione ufficiale no. 6 l'X Consortium, Inc.™ (nel 1996 ribattezzato The Open Group™) ha portato avanti lo sviluppo dell'X Window System.

XFree™ è un'implementazione libera dell' X-server per sistemi PC Unix (vedi `http://www.XFree86.org`); XFree è stato sviluppato e continua ad esserlo da programmatori sparsi in tutto il mondo, che nel 1992 si riunirono nel team XFree. Da questo gruppo nacque la The XFree86 Project, Inc.™, fondata nel 1994, il cui scopo è quello di mettere a disposizione XFree™ ad un vasto pubblico e di contribuire all'ulteriore ricerca e sviluppo dell'sistema X Window.

Per poter usare in maniera ottimale l'hardware a disposizione (mouse, scheda grafica, monitor, tastiera), si ha la possibilità di modificare manualmente la configurazione. Informazioni dettagliate riguardanti la configurazione del sistema X Window si trovano nei diversi file della directory `/usr/share/doc/packages/xf86` e naturalmente anche nella pagina di manuale che potete invocare con `man XF86Config`.

Attenzione

La configurazione del sistema X Window deve venire eseguita con estrema accuratezza. X11 non va inizializzato se prima non si sia terminata la configurazione. Un sistema configurato in maniera errata può causare danni irreparabili all'hardware in particolare a monitor a frequenza fissa. Gli autori di questo libro e la SUSE LINUX AG declinano ogni responsabilità per eventuali danni. Il presente testo è stato redatto e tradotto con la maggiore accuratezza possibile. Ciononostante non si può garantire in modo assoluto che i metodi qui presentati siano corretti e che non possano arrecare dei danni al vostro hardware.

Attenzione

4.1 Come ottimizzare l'installazione del sistema X Window

In questo sezione descriveremo la struttura del file di configurazione `/etc/X11/XF86Config`. Questo file è suddiviso in sezioni (ingl. *sections*) introdotte dalla parola chiave `Section "identificatore"`, e

che terminano con `EndSection`. Ci limiteremo a presentare le sezioni principali.

I programmi SaX2 e xf86config creano il file `XF86 Config` di default in `/etc/X11`. Questo è il file di configurazione primario per l' X Window System. Qui trovate le impostazioni per mouse, monitor e scheda grafica.

`XF86Config`, come già accennato, è composto da più sezioni `Sections`, ognuna delle quali si occupa di un aspetto della configurazione. Una sezione è sempre strutturata nel modo seguente:

```
Section denominazione della sezione
registrazione 1
registrazione 2
registrazione n
EndSection
```

Esistono i seguenti tipi di sezioni:

Tabella 4.1: *Sezioni in /etc/X11/XF86Config*

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 touch tables, joysticks 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 i modeline, possano venire inviate al monitor frequenze troppo alte.

`Modes`	Qui vengono definiti i parametri di rappresentazione delle singole 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. Spiegare dettagliatamente i singoli parametri non rientra nello scopo del presente manuale; 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 con il nome indicato.
`Screen`	Questa sezione infine riunisce un `Monitor` e un `Device` da cui derivare le indicazioni necessarie per XFree. 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 in un'unità i dispositivi d'immessione `InputDevice` e quelli di visualizzazione. `Screen`.

Occupiamoci ora delle sezioni `Monitor`, `Device` e `Screen`. Nella pagina di manuale di `XF86Config` troverete ulteriori informazioni sulle altre sezioni.

Un file `XF86Config` può contenere più sezioni `Monitor` e `Device`. Sono possibili anche più sezioni `Screen`; quale di queste venga usata, dipende dalla sezione successiva `ServerLayout`.

4.1.1 Screen-Section

Diamo un'occhiata alla sezione screen; come già accennato, questa raggruppa le sezioni monitor e device e stabilisce la risoluzione e la profondità dei colori.

Ecco una sezione Screen esempio: 4.1 a fronte.

Exempio 4.1: *La sezione Screen del file /etc/X11/XF86Config*

```
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 alla sezione Device e Monitor con i rispettivi nomi o Identifier. Entreremo nei dettagli riguardanti queste sezioni più avanti.

Tramite l'indicazione `DefaultDepth`, si può scegliere con quale profondità dei colori debba partire il server (se viene inizializzato senza una precisa indicazione della profondità dei colori). 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, in base alla sezione Monitor, una `Modeline` supportata dallo schermo e dalla scheda grafica.

La prima risoluzione in questo senso è quella con la quale parte l'X-server (il cosiddetto `Default-Mode`). Con i tasti Ctrl-Alt-(+) vi spostate a destra, con i tasti Ctrl-Alt-(-) 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.e. la scheda grafica ha 16 MB di video RAM, lo schermo virtuale - con una profondità di colore di 8 bit - può raggiungere fino a 4096x4096(!) pixel. Specialmente con server accelerati non è consigliabile dedicare allo schermo virtuale l'intera memoria della scheda grafica, poiché la memoria inutilizzata viene allocata da questi server per diverse font cache ed alla cache grafica.

4.1.2 Device-Section

Una Device Section descrive e definisce una determinata scheda grafica. `XF86Config` 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, con `Device[0]` la prima, con `Device[1]` la seconda 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 emette le indicazioni in 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 nella sottodirectory `drivers` di `ModulePath` definito nella sezione `Files`. 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 il file driver `mga_drv.o`.

Tramite ulteriori opzioni, è possibile influenzare il comportamento dell'X server o del driver. Nella Device Section, a scopi dimostrativi, è stata settata 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 mode generale si trovano anche nelle rispettivie pagine di manuale (`man XF86Config` e `man XFree86`).

4.1.3 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/XF86Config` 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 in cui vengono indicati 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.

Attenzione

Senza cognizioni di base sul funzionamento di monitor e scheda grafica, le modeline non dovrebbero venire modificate, poiché ciò potrebbe danneggiare seriamente il vostro monitor!

Attenzione

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 [16], in cui vengono descritte la funzione dell'hardware e la creazione delle modeline.

Fortunatamente, diventano sempre più rari i casi in cui bisogna impostare manualmente la 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.

4.2 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 (vedi la sezione 4.2.1 a pagina 88), e per fare in modo che i font siano utilizzabili anche tramite il nuovo sistema di font rendering Xft anche in una sottodirectory delle directory configurate in `/etc/fonts/fonts.conf` (vedi la sezione 4.2.1 a fronte).

I file del font possono essere copiati in una directory indicata come utente `root` manualmente per esempio in `/usr/X11R6/lib/X11/fonts/truetype/`, oppure potrete utilizzare per fare ciò 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 4.2.1 a pagina 89.

4.2.1 Dettagili sui sistemi di font

XFree contiene due completamente differenti sistemi di font, il vecchio *sistema di font X11 Core* ed il nuovo sistema *Xft/fontconfig*. Segue una breve descrizione dei due sistemi.

Xft

In fase di ideazione di Xft si è dedicata particolare attenzione al supporto di font scalabili, incluso l'anti-aliasing. Con Xft i font vengono modificati dal programma che utilizza i font e non dal 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 controllo sui particolari ad es. come modificare i glifi. Questo permette la rappresentazione corretta di testo nelle varie lingue, ed inoltre l'accesso diretto ai file di font è di aiuto per integrare (ingl. *to embed*) font per il processo di stampa affinché quando emesso allo schermo corrisponda effettivamente a quanto emesso dalla stampante.

I due ambienti desktop KDE e Gnome, Mozilla e tante altre applicazioni utilizzano già sotto SUSE LINUX Xft di default. Quindi, Xft viene utilizzato già da più applicazioni che vecchio sistema di font X11 Core.

Xft utiizza la libreria Fontconfig per trovare i font e per influire sul modo nel quale verranno modificati. 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 directrory 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 disattivar 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 adatto.

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 lo minimo sforzo ottenete 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`.

`fc-list ""` emette un elenco con tutti i font. Se volete sapere quali sono i font scalabili a vostra disposizione (`:outline=true`) che includono tutti i glifi richiesti per l'ebraico (`:lang=he`) e per tutti i font volete avere il nome di font (`family`), stile (`style`), grado di grassetto (`weight`) e nome di file del font, immette ad esempio il seguente commando:

```
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 4.2: *Possibili parametri di fc-list*

Parametri	Significato e valori possibili
family	Il nome della famiglia di font ad esempio `FreeSans`
foundry	I produttori di 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 di file sotto quale è stato salvato 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 sensato solo per font bitmap.

Font X11 Core

Oramai il sistema di font X11 Core non supporto solo font bitmap, ma anche font scalabili come font Type1, TrueType/OpenType e font CID-keyed. Anche font Unicode vengono supportato già da parecchio tempo.

Nel 1987 il sistema di font X11 Core è stato sviluppato per X11R1 per poter elaborare font bitmap monocromatici ed ancora oggi che tutte le estensioni menzionati sopra sono stati aggiunti in un secondo momento.

Ad esempio vi è il supporto per font scalabili solo senza antialiasing e subpixel rendering, e caricare font estesi, scalabili con tanti glifi per numerose lingue può rilevarsi essere un processo molto lento. Anche l'utilizzo di font unicode può richiedere molto tempo e consuma più memoria di quanto non fosse necessario.

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 e non più estensibile in modo sensato. Comunque per motivi di compatibilità verso il basso rimane disponibile, ma dove possibile si dovrebbe utilizzare il sistema più moderno Xft/fontconfig.

Tenete presente che vengono considerati dall' X server solo directory che

- nella sezione `Files` del file `/etc/X11/XF86Config` sono registrati come `FontPath`.
- hanno un file `font.dir` valido (viene creato da SuSEconfig).

- non sono state disconnesse con l'X server in esecuzione tramite il comando `xset -fp`.
- oppure sono state integrate con l'X server in esecuzione tramite il comando `xset +fp`.

Se l' X server è già in esecuzione potete rendere disponibili font appena installati nelle directory integrate 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 `sux` seguito dall'immissione del password di root in un terminale per diventare `root`, `sux` 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 che sono disponibili tramite il sistema di font X11 Core utilizzate il comando `xlsfonts` che elenca tutti i font disponibili.

SUSE LINUX utilizza di default UTF-8 Locales, quindi dovreste utilizzare font Unicode che si riconoscono dalla desinenza `iso10646-1` del nome di font elencato da `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 prima si utilizzava l'encoding `iso-8859-*`.

Font CID-keyed

A differenza di altri tipi di font, nel caso di font CID-keyed non possono essere installati in una directory qualunque, dovrebbere essere in ogni caso essere installati in `/usr/share/ghostscript/Resource/CIDFont/`. Questo non fa differenza per Xft/fontconfig, ma lo richiedono Ghostscript ed il sistema di font X11 Core.

Nota

Per ulteriori informazioni in tema di font sotto X11 consultate `http://www.xfree86.org/current/fonts.html`.

Nota

4.3 Configurare OpenGL/3D

Quale interfaccia 3D Linux offre l'interfaccia OpenGL. Direct3D della Microsoft non è disponibile sotto Linux.

4.3.1 Supporto hardware

SUSE LINUX contiene molti driver OpenGL per il supporto hardware 3D. Ecco una rassegna nella tabella 4.3.

Tabella 4.3: *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 Matrox G200/G400/G450/G550 ATI Rage 128(Pro)/Radeon

Se effettuate l'installazione tramite YaST, potete attivare il supporto 3D durante l'installazione, se il relativo supporto viene rilevato da YaST, fatta eccezione per i chip grafici nVidia. Per questi chip, si dovrà installare 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 possiamo fornire il driver nVidia.

Se avete eseguito un update, il supporto di hardware 3D va impostato in modo diverso. La procedura da seguire dipende dal driver OpenGL utilizzato e verrà descritta in dettaglio nella sezione seguente.

4.3.2 Driver OpenGL

nVidia e DRI

Questi driver OpenGL possono essere configurati comodamente con SaX2. Tenete presente che se siete in possesso di una scheda nVidia dovete prima installare il driver nVidia (vedi sopra). Con il comando `3Ddiag`, potete controllare se la configurazione di nVidia o DRI sia corretta.

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 verrà usato il *Software Rendering Fallback* del driver OpenGL che è molto lento. Usate il comando `id` per controllare se l'utente attuale appartiene al gruppo `video`. Se non appartiene al gruppo, potete usare YaST per aggiungere l'utente al gruppo.

4.3.3 Tool di diagnosi 3Ddiag

Per controllare la configurazione 3D su SUSE LINUX, è disponibile lo strumento di diagnosi 3Ddiag. Si tratta di uno strumento a riga di comando che deve essere invocato da un terminale.

Questa applicazione può esaminare, per esempio, la configurazione di XFree86, verificare se i pacchetti per il supporto 3D siano installati e se viene usata la corretta libreria OpenGL nonché l'estensione GLX. Seguite le istruzioni di 3Ddiag se appaiono i messaggi "failed". Se tutto è andato per il verso giusto dovreste vedere allo schermo solo messaggi "done".

Con `3Ddiag -h` potete vedere le opzioni ammesse per 3Ddiag.

4.3.4 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 eseguiti in modo fluido su un computer relativamente recente. Per vedere se l'accelerazione 3D è abilitata o meno, date un'occhiata all'output di `glxinfo`: in tal caso `direct rendering` deve essere impostato su `Yes`.

4.3.5 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 XFree86. Spesso troverete la riga `DRI is disabled` in `/var/log/XFree86.0.log` di XFree86. La causa esatta dei problemi può essere scoperta 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.

4.3.6 Supporto all'installazione

A parte il Software Rendering Fallback del driver DRI, in Linux tutti 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 X11 non include la configurazione dell'accelerazione hardware 3D. Speriamo comunque che questo capitolo fornisca una risposta a molte delle domande relative a questo argomento. Se avete delle difficoltà con il supporto hardware 3D, consigliamo in caso di dubbio di rinunciare al supporto 3D.

4.3.7 Ulteriore documentazione in linea

- DRI: `/usr/X11R6/lib/X11/doc/README.DRI` (il `XFree86-doc`)

Processo di stampa

Questo capitolo riassume i principi fondamentali della stampa in Linux. Gli esempi consentiranno di capire i nessi del processo di stampa che a sua volta permetterà di trovare il giusto approccio per risolvere delle eventuali difficoltà più celermente.

5.1 I principi del processo di stampa

In Linux le stampanti vengono indirizzate attraverso cosiddette *code di stampa* (print queue). I dati da stampare vengono memorizzati temporaneamente nella coda di stampa da dove lo spooler della stampante li inoltrerà alla stampante.

Spesso i dati da stampare non si trovano nel formato da poter essere inviati direttamente alla stampante. Una grafica per esempio di solito deve essere convertita in un formato che può essere emesso direttamente dalla stampante. Il cosiddetto *filtro della stampante* traduce i dati da stampare in un linguaggio compreso dalla stampante.

5.1.1 Esempi di linguaggi di stampante standard

Testo ASCII La maggior parte delle stampanti emette direttamente almeno testo in ASCII. Le stampanti che rappresentano una delle poche eccezioni non in grado di stampare direttamente testi in ASCII, vengono indirizzate da uno dei seguenti linguaggi di stampante standard.

PostScript *PostScript* è il linguaggio standard di Unix/Linux, che permette di stampare direttamente su stampanti PostScript. Queste stampanti sono relativamente costose, visto che PostScript è un linguaggio potentissimo ma complesso che causa un elevato workload nella stampante Post-Script per produrre un copia stampata. Inoltre a causa della licenza si creano dei costi aggiuntivi.

PCL3, PCL4, PCL5e, PCL6, ESC/P , ESC/P2 e ESC/P a matrice
Se non vi è una stampante PostScript, il filtro della stampante ricorre al programma Ghostscript per convertire i dati in uno di questi linguaggi di stampante standard. Viene utilizzato un driver Ghostscript adatto il più possibile al modello della stampante, in modo da considerare le particolarità del modello, per esempio le impostazioni del colore.

5.1.2 Il processo di stampa

1. L'utente o un'applicazione crea un incarico di stampa.

2. I dati da stampare vengono memorizzati temporaneamente nella coda di stampa da dove lo spooler della stampante li inoltra al filtro della stampante.

3. Normalmente il filtro della stampante fa quanto segue:

   (a) Determina il tipo dei dati da stampare.

   (b) Se i dati da stampare non sono di natura PostScript, vengono innanzitutto convertiti nel linguaggio standard PostScript. In particolare testi ASCII vengono convertiti in PostScript.

   (c) I dati PostScript vengono convertiti eventualmente in un altro linguaggio di stampante.

   - Se è collegata una stampante PostScript, i dati PostScript vengono inviati direttamente alla stampante (o ad un'altra coda di stampa). Eventualmente vengono invocate le funzioni della bash `duplex` e `tray`, definite in `/usr/lib/lpdfilter/global/functions` per consentire la stampa duplex o di selezionare il cassetto della carta tramite dei comandi PostScript— ammesso che la stampante PostScript sia in grado di elaborare questi comandi.
   - Se non vi è collegata alcuna stampante PostScript Ghostscript viene utilizzato con un driver Ghostscript adatto al relativo modello di stampante per generare i dati specifici da stampare da inviare alla stampante (o ad un'altra coda di stampa).

   I parametri relativi alla stampante per i comando Ghostscript sono memorizzati in uno dei seguenti file:

   - Nel file /etc/printcap direttamente nella riga "cm".
   - Direttamente nel file `/etc/lpdfilter/coda_di_stampa/upp` (laddove ⟨*coda_di_stampa*⟩ va sostituito con il vero nome della coda di stampa).
   - In modo indiretto nel `file/etc/lpdfilter/coda_di_stampa/ppd` (laddove ⟨*coda_di_stampa*⟩ va sostituito con il nome effettivo della coda di stampa). Se l'lpdfilter è stato configurato con YaST la conversione dei dati nel formato della stampante avviene in modo analogo al sistema di stampa CUPS con filtro foomatic-rip, che crea il comando Ghostscript relativo alla stampante dai dati dello stesso file PPD Foomatic che è stato utilizzato anche per il sistema di stampa CUPS.

Eventualmente è possibile riformattare l'output di Ghostscript, se vi è un relativo script sotto /etc/lpdfilter/coda_stampa/post (laddove coda di stampa va sostituito con l'effettivo nome della coda di stampa).

4. Dopo che l'incarico di stampa è stato inviato completamente alla stampante, lo spooler della stampante cancella l'incarico dalla coda di stampa.

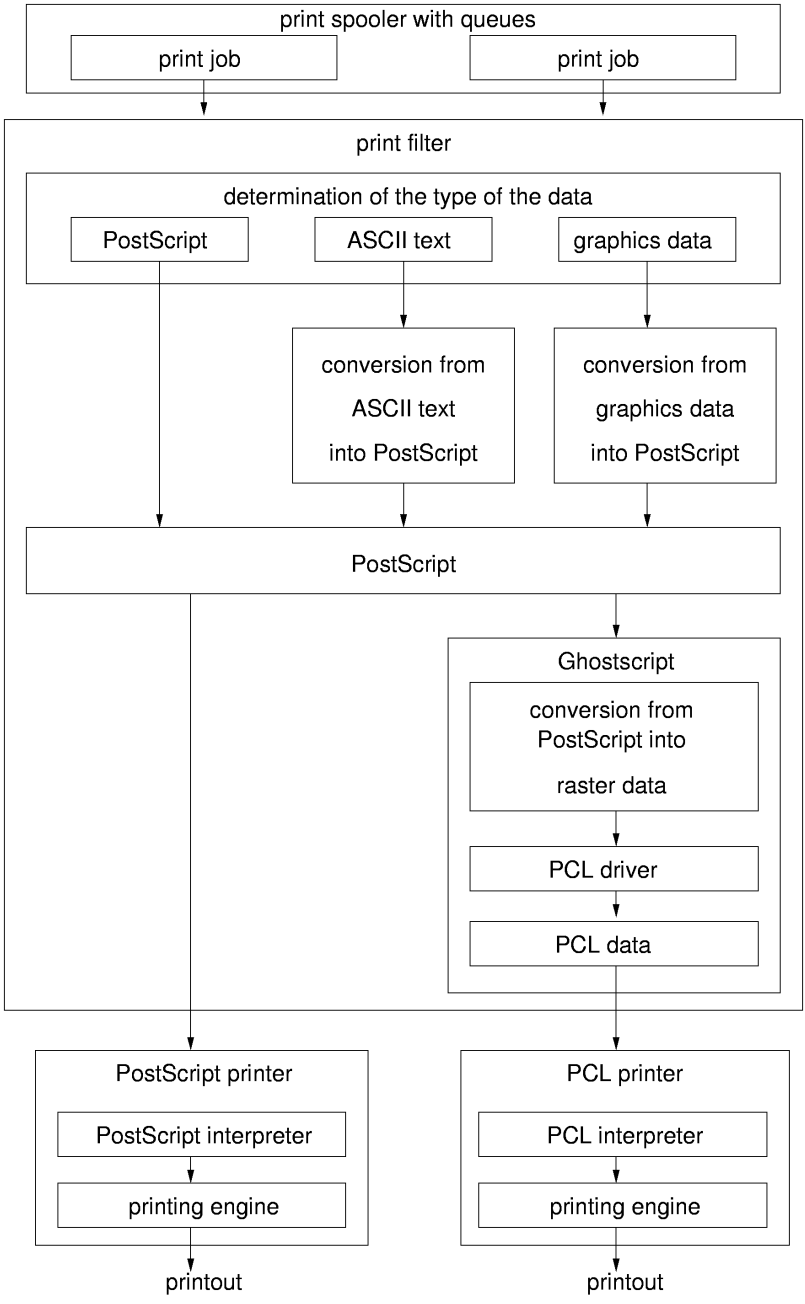

Figura 5.1: *Rassegna del processo di stampa*

5.1.3 Diversi sistemi di stampa

SUSE LINUX supportata due diversi sistemi di stampa:

LPRng/lpdfilter Si tratta di un sistema di stampa tradizionale composto da uno spooler di stampante LPRng e di un filtro di stampante lpdfilter. Nei sistemi di stampa tradizionali la configurazione delle code di stampa viene stabilita dall'amministratore di sistema, ed l'utente può scegliere tra le diverse code di stampa. Al fine di poter scegliere tra diverse configurazioni per una stampante, si devono impostare diverse code di stampa con configurazioni diverse per la stessa stampante. Con le semplici stampanti monocromatiche (p.e. la maggior parte delle stampanti laser) basta una configurazione standard, ma per le moderni stampanti a getto di inchiostro a colori servono configurazioni per stampe monocromatiche, a colori ed eventualmente per stampe policrome ad alta risoluzione nonché fotostampe. Attraverso le configurazioni stabilite, da una parte, viene assicurato che vengano utilizzate solo le configurazioni impostate dall'amministratore di sistema, dall'altra però viene preclusa ogni possibilità all'utente di eseguire una qualunque impostazione personale. Per l'amministratore di sistema questo significa dover impostare di conseguenza tante code di stampa, se deve essere reso disponibile l'elevato numero delle funzionalità proprie delle stampanti di ultima generazione.

CUPS Nel sistema di stampa CUPS l'utente ha la possibilità di stabilire impostazioni specifiche della stampante per ogni incarico di stampa. In tal modo, la configurazione della coda di stampa non viene stabilita per intero dall'amministratore di sistema, ma le possibilità di impostazioni specifiche della stampante sono deposte per ogni coda di stampa in un file sì detto PPD *PostScript Printer Description* che vengono proposte all'utente in una finestra di dialogo della stampante. Le varie possibilità offerte dalla stampante sono deposte nel file PPD; l'amministratore di sistema può comunque modificare il file PPD ed eventualmente limitare le possibilità di configurazione.

Poiché i due sistemi di stampa sono in conflitto, di solito non è possibile installare entrambi i sistemi di stampa *contemporaneamente*; YaST2 comunque permette di passare dall'uno all'altro sistema di stampa – vedi nel *Manuale dell'utente* la sezione *YaST — Configurazione, Stampante*.

5.2 Premesse per stampare

5.2.1 Premesse generali

- La stampante viene supportata da SUSE LINUX? Vedi a riguardo anche le seguenti fonti di informazione:

  Banca dati SUSE delle stampanti
  `http://cdb.suse.de` oppure `http://hardwaredb.suse.de/`

  Banca dati delle stampanti Linuxprinting.org
  `http://www.linuxprinting.org/` (The Database `http://www.linuxprinting.org/database.html` o l'elenco `http://www.linuxprinting.org/printer_list.cgi`)

  Ghostscript `http://www.cs.wisc.edu/~ghost/`

  Driver Ghostscript SUSE LINUX
  `file:/usr/share/doc/packages/ghostscript/catalog.devices`. Qui sono elencati i driver Ghostscript che sono effettivamente inclusi nella relativa versione di SUSE LINUX. Questo è importante, poiché a volte su Internet viene indicato un driver Ghostscript non incluso in SUSE LINUX. In SUSE LINUX è accluso per motivi di licenza GNU Ghostscript. Di solito vi è anche un driver Ghostscript GNU con il quale la stampante funziona.

- La stampante è fondamentalmente indirizzabile; vedi la sezione 5.3.4 a pagina 106.

- Dovreste utilizzare un kernel originale SUSE che trovate sui CD-ROM, *non* utilizzate dunque un kernel compilato da voi. In caso di problemi dovreste installare un kernel SUSE originale ed eseguire con questo il reboot.

- Vi raccomandiamo l'installazione del 'Sistema standard' con YaST2, per assicurare che tutti i pacchetti necessari siano disponibili. E' bene durante l'installazione del sistema standard non deselezionare pacchetti preselezionati. Altrimenti installate almeno il 'Sistema standard'. Il 'sistema minimale' non basta per stampare.

5.2.2 Determinare il driver adatto alla stampante

La stampante PostScript non necessita di speciali driver. Vedi a riguardo la sezione 5.1.2 a pagina 94. Un driver PostScript genera per stampanti non PostScript i dati specifici di stampa. Per tale ragione è il driver Ghostscript a determinare il risultato stampato emesso da stampanti non PostScript. La scelta del driver Ghostscript ed eventualmente particolari impostazioni relativi al driver influiscono sul risultato del processo di stampa. Gli elenchi di cui nella sezione 5.2.1 nella pagina precedente indicano anche driver Ghostscript per i singoli modelli di stampante.

Se non trovate alcun driver Ghostscript per la vostra stampante chiedete eventualmente al produttore della stampante, quale sia il linguaggio della vostra stampante. Alcuni produttori mettono a disposizione dei driver Ghostscript speciali per il proprio modello di stampante. Se il produttore non è in grado di fornirvi delle informazioni in tema di Linux può comunque aiutarvi a trovare il driver giusto fornendo le seguenti informazioni:

- Verificate se la vostra stampante è compatibile con un modello che gira sotto Linux e utilizzate il driver Ghostscript del modello compatibile. Linux compatibile significa che la vostra stampante utilizzando le stesse sequenze di controllo binarie riesce a stampare correttamente come il modello compatibile –, cioè la stampante comprende lo stesso linguaggio in modo diretto e non ha bisogno di un driver adatto che lo emula (per un altro sistema operativo).

  La similitudine nella denominazione delle stampanti, non comporta l'esistenza di una compatibilità. Questo è dovuto al fatto che, a volte, stampanti con una denominazione simile, non comprendono lo stesso linguaggio.

- Quale sia il linguaggio compreso direttamente dalla vostra stampante ve lo potrà dire il produttore. Nel manuale della stampante, tra i dati tecnici, spesso viene indicato il linguaggio della stampante.

  PCL5e o PCL6 Stampanti che comprendono *PCL5e* o *PCL6* senza intermediazione, dovrebbero funzionare con il driver Ghostscript ljet4 fino a 600x600 dpi. Spesso PCL5e viene indicato solo con PCL5.

  PCL4 o PCL5 Stampanti che comprendono direttamente *PCL4* o *PCL5* dovrebbero funzionare con uno dei seguenti driver Ghostscript: laserjet, ljetplus, ljet2p o ljet3; comunque sono limitati a 300x300 dpi.

PCL3 Stampanti che riescono ad elaborare direttamente *PCL3* dovrebbero funzionare con i driver Ghostscript deskjet, hpdj, pcl3, cdjmono, cdj500 o cdj550.

ESC/P2, ESC/P o ESC/P a matrice
Stampanti che comprendono direttamente *ESC/P2*, *ESC/P* o *ESC/P* a matrice dovrebbero funzionare con i driver Ghostscript uniprint assieme ad un file parametro adatto `.upp` (p.e. `stcany.upp`).

5.2.3 Stampanti GDI

Dato che i driver delle stampanti per Linux di solito non vengono sviluppati dal produttore dell'hardware, per indirizzare la stampante bisogna ricorrere ad un linguaggio generalmente compreso come *PostScript*, *PCL* e *ESC/P*. Una stampante normalmente comprende almeno uno dei linguaggi comunemente usati. Se però il produttore crea una stampante che può essere indirizzata solo con proprie particolari sequenze di controllo, ci troviamo di fronte ad una cosiddetta *stampante GDI* che funziona solo con la versione del sistema operativo per la quale il produttore acclude il driver. Visto che il modo di indirizzare questo tipo di stampanti non corrisponde a nessuna delle norme note, non è possibile, o solo accompagnato da tante difficoltà, utilizzare sotto Linux questi dispositivi fuori dalla norma.

GDI è una interfaccia di sviluppo concepita dalla Microsoft per la rappresentazione grafica. Il problema non è rappresentato dall'interfaccia di programmazione ma dal fatto che le cosiddette stampanti GDI possono essere indirizzate *solo* attraverso il linguaggio proprietario del relativo modello di stampante. In fondo l'espressione stampante indirizzabile *solo* attraverso un linguaggio di stampante proprietario, sarebbe più corretta.

Ve ne sono alcune, che oltre al modo GDI - previa configurazione - comprendono anche un linguaggio standard. Se accanto ad Linux utilizzate anche un altro sistema operativo, il driver della stampante di quest'ultimo potrà avere innescato eventualmente la modalità GDI della stampante, in modo da rendere impossibile il funzionamento sotto Linux. Avete due possibilità: riportate la stampante - sotto il sistema operativo installato accanto ad Linux - alla modalità standard, oppure utilizzate - anche sotto l'altro sistema operativo - la stampante solo nella modalità standard, che spesso però comporta una restrizione delle funzionalità della stampante (p.e. una risoluzione minore).

Vi sono inoltre delle particolari stampanti che comprendono solo parti rudimentali del linguaggio standard - per esempio solo comandi per l'emissione di dati di grafici a matrice. Questo tipo di stampante a volte può essere utilizzato del tutto normalmente, poiché tanti driver Ghostscript di solito utilizzano solo comandi per l'emissione di dati di grafici a matrice. Eventualmente dei testi in ASCII non potranno essere stampati direttamente dalla stampante ma di default verrà sempre frapposto Ghostscript. I problemi con questo tipo di stampanti sorgono solo, se si deve cambiare il modo della stampante con delle sequenze di controllo particolari. In questo caso non potete utilizzare un driver Ghostscript comune, serve invece un driver adatto con cui è possibile eseguire questo passaggio.

Per alcune stampanti GDI esistono propri driver della casa produttrice. Lo svantaggio di questi driver Linux *per stampanti GDI* è che non può essere garantito il funzionamento con diverse (future) versioni di Linux.

Stampanti comprendenti un linguaggio di stampa standard che è stato pubblicato, non dipendono invece né da un particolare sistema operativo né da particolari versioni di un sistema operativo, e spesso sono i driver Linux messi a disposizione dei produttori per questo tipo di stampanti a produrre i migliori risultati.

Le seguenti stampanti GDI sono supportate direttamente da SUSE LINUX e per mezzo di YaST2 potrete configurarle; visto che comunque le stampanti GDI causano spesso dei problemi, può accadere che alcuni modelli non funzionano o vi sono delle vistose restrizioni (p.e. solo stampa in bianco e nero a bassa risoluzione). Tenete presente che non possiamo garantire l'affidabilità delle indicazioni che seguono, poiché non testiamo driver di stampanti GDI.

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

Sono almeno le seguenti stampanti GDI che da quanto abbiamo potuto appurare *non* vengono supportate da SUSE LINUX, ma questo elenco non è completo:

- Brother DCP-1000, MP-21C, WL-660
- Canon BJC 5000,5100,8000,8500, LBP 460,600,660,800, MultiPASS L6000
- Epson AcuLaser C1000, EPL 5500W,5700L,5800L
- HP LaserJet 1000,3100,3150
- Lexmark Z12,22,23,31,32,33,82, Winwriter 100,150c,200
- Minolta PagePro 6L,1100L,18L, Color PagePro L, Magicolor 6100DeskLaser, Magicolor 2 DeskLaser Plus/Duplex
- Nec SuperScript 610plus,660,660plus
- Oki Okijet 2010
- Samsung ML 85G,5050G, QL 85G
- Sharp AJ 2100, AL 1000,800,840,F880,121

5.3 Configurare la stampante con YaST

5.3.1 Code di stampa e configurazioni

Solitamente sono necessarie più code di stampa per i seguenti motivi:

- Stampanti differenti devono essere indirizzate attraverso code di stampa differenti.
- Per ogni coda di stampa si può configurare il filtro di stampa in modo mirato. Si utilizzano diverse code di stampa per una stessa stampante per avere a disposizione diverse configurazioni. Con CUPS questo non è necessario poiché l'utente ha qui la possibilità di stabilire da sè le relative impostazioni; si veda a riguardo la sezione 5.1.3 a pagina 98.

Con stampanti in bianco e nero (p.e. la maggioranza delle stampanti laser) basta una configurazione standard, ma per stampanti a getto di inchiostro policrome servono almeno due tipi di configurazione — e di conseguenza due code di stampa:

- Una configurazione standard per una stampa veloce e non particolarmente costosa in bianco e nero.
- Una configurazione color ovvero una coda di stampa per stampe a colori.

5.3.2 I principi della configurazione della stampante con YaST

Il modulo di configurazione della stampante di YaST può essere richiamato oltre che attraverso i menu, anche dall'utente `root` direttamente dalla riga di comando con `yast2 printer`.

Passare da CUPS e LPRng/lpdfilter è facile grazie ad un menu speciale della configurazione della stampante di YaST tramite il bottone 'Per esperti'. Durante il passaggio però si perde una delle configurazioni esistenti, cioè una configurazione CUPS non viene convertita in una LPRng/lpdfilter o viceversa.

Nel modulo di configurazione della stampante in YaST avete la scelta tra i seguenti sistemi di stampa ed avete modo di eseguire il passaggio da un sistema di stampa all'alltro.

CUPS come server (default nella installazione standard)
Con una stampante collegata in locale, CUPS deve girare come server. Se non viene impostata alcuna coda di stampa locale tramite YaST il demone CUPS cupsd non verrà lanciato automaticamente. Se cupsd deve venire eseguito comunque, si dovrà abilitare il servizio 'cups' (normalmente per i runlevel 3 e 5) – vedi la sezione 5.8.2 a pagina 123. In particolar modo vengono installati per questo sistema di stampa i seguenti pacchetti:

- `cups-libs`
- `cups-client`
- `cups`
- `footmatic-filters`
- `cups-drivers`
- `cups-drivers-stp`

CUPS esclusivamente come client Se nella rete locale vi è un server di rete CUPS, (vedi la sezione 5.8.1 a pagina 122) e se si intende stampare

solo attraverso le sue code di stampa, è sufficiente che CUPS giri solo come client. Vedi la sezione 5.8.2 a pagina 123. A tal fine bastano i seguenti pacchetti:

- `cups-libs`
- `cups-client`

LPRng Se volete usare il sistema di stampa LPRng/lpdfilter o se nella rete vi è solo un server LPD (vedi sezione 5.8.1 a pagina 122) e si intende stampare attraverso le sue code di stampa – vedi la sezione 5.8.2 a pagina 123 ed installate i seguenti pacchetti:

- `lprng`
- `lpdfilter`
- `footmatic-filters`
- `cups-drivers`

`cups-client` e `lprng` si escludono a vicenda e non possono essere installati insieme. `cups-libs` deve essere installato in ogni caso, poiché alcuni programmi (p.e. `Ghostscript`, `KDE`, `Samba`, `Wine` ed il modulo di configurazione della stampante di YaST) necessitano le librerie CUPS.

Per un sistema di stampa completo servono di solito ulteriori pacchetti che comunque con 'Sistema standard' vengono installati automaticamente:

- `ghostscript-library`
- `ghostscript-fonts-std`
- `ghostscript-x11`
- `libgimpprint`

La configurazione della stampante con YaST indica le configurazioni generate correttamente.

Dato che la configurazione viene generata effettivamente solo dopo aver concluso la configurazione della stampante YaST, ai fini di un controllo si dovrebbe riavviare la configurazione della stampante eseguita con YaST2.

5.3.3 Configurazione automatica

A seconda della misura nella quale YaST rivela automaticamente l'hardware e della misura nella quale nella banca dati delle stampanti sono presenti informazioni relative alla stampante in questione, YaST è in grado di determinare automaticamente i dati necessari ai fini della configurazione o proporne una da assumere; altrimenti l'utente dovrà inserire i dati richiesti nei dialoghi. YaST consente la configurazione automatica della stampante, se vengono soddisfatte le seguenti condizioni:

- Durante la rivelazione automatica dell'hardware, la porta parallela o la porta USB è stata impostata correttamente e la stampante ad essa collegata è stata rilevata automaticamente.
- Nella banca dati della stampante vi è l'ID del modello della stampante, che YaST ha ottenuto durante il rilevamento automatico dell'hardware. Visto che questo ID può discostarsi dalla denominazione del modello, può darsi che il modello dovrà essere selezionato manualmente.

Per ogni tipo di configurazione si consiglia di eseguire un test di stampa con YaST per verificarne il corretto funzionamento, anche perché in molti casi si devono utilizzare dei dati di configurazione senza supporto esplicito da parte del produttore, ed in tal modo non è possibile dare delle garanzie per ogni dato.

Inoltre il test di stampa con YaST fornisce importanti informazioni sulla relativa configurazione.

5.3.4 Configurazione manuale

Nel caso in cui anche solo una delle premesse per la configurazione automatica non venisse soddisfatta o se si desidera un tipo di configurazione particolare - per così dire "su misura" - le impostazioni vanno eseguite manualmente, e si dovrà configurare:

Connessione dell'hardware (porta)

- Se YaST rivela automaticamente il modello di stampante, si può presumere che la connessione della stampante funziona a livello dell'hardware, e che dunque non bisognerà procedere con l'impostazione.

- Se però YaST non rivela automaticamente il modello della stampante, ciò indica che la connessione della stampante funziona a livello dell'hardware solo previa configurazione manuale. Configurando manualmente si deve scegliere la porta. `/dev/lp0` è la prima porta parallela. `/dev/usb/lp0` è la porta per una stampante USB. In questi casi va assolutamente eseguito il relativo test in YaST per controllare se la stampante è indirizzabile attraverso la porta selezionata.

  Il modo più sicuro in questi casi è connettere la stampante direttamente alla prima porta parallela e settare nel BIOS le seguenti impostazioni per la porta parallela:

  - Indirizzo IO `378` (esadicimale)
  - L'interrupt non è rilevante
  - Modo `Normal`, `SPP` oppure `Output-Only`
  - Senza DMA

  Se nonostante queste impostazioni nel BIOS la stampante non risulta essere indirizzabile attraverso la prima porta parallela, allora nelle impostazioni dettagliate per la porta parallela deve essere inserito in modo esplicito l'indirizzo IO `0x378` - in corrispondenza alle impostazioni nel BIOS. Se esistono due porte parallele impostate sugli indirizzi IO `378` e `278` (esadecimale), allora devono essere inserite nel seguente modo: `0x378,0x278`.

Nome della coda di stampa Dato che spesso va indicato il nome della coda di stampa per stampare, usate solo nomi brevi composti da minuscole ed eventualmente cifre.

Driver Ghostscript o linguaggio della stampante (modello della stampante)

Il driver Ghostscript e linguaggio della stampante vengono determinati dal modello della stampante e vengono stabiliti attraverso la scelta di una configurazione predefinita, che all'occorrenza si lascia modificare in una maschera a parte, cioé selezionando il produttore ed il modello, si seleziona in fondo il linguaggio della stampante od un driver Ghostscript adatto alla stampante con impostazioni di driver predefinite anche esse confacenti.

Dato che il driver Ghostscript genera dati da stampare per stampanti non PostScript, la configurazione del driver Ghostscript è il punto cruciale per determinare il tipo di stampa. In primo luogo è la scelta del driver Ghostscript a determinare le caratteristiche della stampa

ed in secondo luogo le impostazioni driver adatte. Qui vengono impostate le caratteristiche e le differenze che risulteranno nella copia di stampa emessa dalla stampante in base al tipo di configurazione.

Se YaST ha rilevato automaticamente il modello della stampante o il modello è incluso nella banca dati delle stampanti, vi è una preselezione di driver Ghostscript adatti. In questo caso YaST mette a disposizione diversi tipi di configurazione predefiniti – p.e.

- Stampa in bianco e nero
- Stampa a colori a 300 dpi
- Fotostampa a 600 dpi

La configurazione predefinita contiene un driver Ghostscript adatto ed eventualmente impostazioni driver adatti al tipo di stampa in questione.

Nel caso vi siano impostazioni specifiche del driver, le potete modificare in una maschera a parte. Cliccate su un valore e se vi è una sottoselezione, le rispettive voci di menu sono indentate. Non tutte le combinazioni di singole impostazioni di driver tra cui potete scegliere, funzionano in modo indiscriminato con ogni modello di stampante – soprattutto in combinazione con una elevata risoluzione:

Consigliamo vivamente di eseguire un test di stampa con YaST. Se questo tentativo non dovesse produrre il risultato atteso (p.e. tanti fogli quasi vuoti), potete fermare il processo di stampa togliendo tutti fogli ed interrompendo quindi il test. A volte, in seguito non è più possibile stampare. Dunque è meglio interrompere il test e lasciare che il foglio in fase di stampa venga emesso. Se il modello della stampante non è contenuto nella banca dati, avete comunque una selezione di driver Ghostscript generici per linguaggi di stampante standard che trovate sotto Produttore generico.

Altre impostazioni speciali Potete intervenire su queste impostazioni tramite un procedimento particolare e in caso di dubbio conviene non modificare le impostazioni di default. Per il sistema di stampa *CUPS* vi sono le seguenti impostazioni:

- Restrizione d'accesso per determinati utenti.
- Stato della coda di stampa: se concludere il processo di stampa o meno; se la coda di stampa debba accettare incarichi di stampa o meno.

- Pagine con banner o frontespizi: se e quali pagine con banner debbano essere stampate prima o dopo l'incarico di stampa vero e proprio.

Nel caso del sistema di stampa *LPRng/lpdfilter* vi sono le seguenti impostazioni speciali a prescindere dall'hardware:

- Si può stabilire il layout della pagina per la stampa di testi ASCII, non però per grafiche e documenti generati con particolari applicativi.
- Per casi particolari la coda di stampa può essere impostata quale coda sì detta `ascii` che forza il filtro della stampante ad emettere testo ASCII. Questo è necessario per forzare, nel caso di file di testo ASCII non rilevati dal filtro come tali, l'emissione di testo ASCII (p.e. per stampare i sorgenti di PostScript).
- La codificazione nazionale riguarda la raffigurazione di caratteri speciali quando si stampano testi ASCII e testo semplice nelle pagine HTML di Netscape.

5.4 Configurazione per applicativi

Gli applicativi utilizzano code di stampa esistenti come per il processo di stampa dalla riga di comando. Per tale ragione negli applicativi sono le code di stampa esistenti ad essere configurate e non la stampante.

Dalla riga di comando si stampa con il seguente comando:

```
lpr -Pcolor <nome file>
lp -d color <nome file>
```

laddove ⟨*nome file*⟩ va sostituito con il nome del file da stampare. Con l'opzione `-P` oppure `-d` potete determinare esplicitamente la coda di stampa. Con `-P color` o `-d color` viene utilizzata la coda di stampa `color`.

Spesso gli applicativi includono le code di stampa esistenti nei menu di stampa, in modo che non sia necessaria alcuna configurazione aggiuntiva; altrimenti si dovrà spesso immettere o configurare un comando di stampa nell'applicativo. Di solito si tratta del comando di cui sopra senza l'indicazione del ⟨ *nome file* ⟩, quindi `lpr -P color` o `lp -d color`.

5.5 Il sistema di stampa CUPS

5.5.1 Terminologia

Con *client* o *programma client* si indica un programma che viene inizializzato per inviare degli incarichi di stampa al demone di stampante. In questo contesto un *demone di stampante* è un servizio locale che riceve gli incarichi da stampare e li inoltra o li elaborare. Un *server* è un demone che fornisce a una o più stampante i dati da stampare. Ogni server ha contemporaneamente la funzione di un demone. Di solito non viene differenziato né da coloro che usano CUPS né dagli sviluppatori di CUPS tra i termini *server* e *demone*.

5.5.2 IPP e server

Gli incarichi di stampa vengono inviati tramite programmi basati su CUPS come `lpr`, `kprinter` o `xpp`, e tramite l'*Internet Printing Protocol*, abbreviato con IPP, definito negli Internet Standard RFC-2910 e RFC-2911 (vd. `http://www.rfc-editor.org/rfc.html`). L' IPP è simile al protocollo Web HTTP: presenta gli stessi header, ma diversi dati utente. Viene utilizzata anche un'altra, propria porta 631 ai fini della comunicazione, registrata comunque presso l' IANA *Internet Authority for Number Allocation*.

I dati vengono inviati al demone CUPS configurato, che normalmente è anche il server locale. Altri demoni possono ad esempio essere indirizzati direttamente tramite la variabile di shell `CUPS_SERVER`.

Tramite la funzione Broadcast del demone CUPS possono essere comunicate alla rete le stampanti amministrate localmente dal demone (porta UDP `631`) in modo che tutti i demoni che ricevono e possono analizzare (configurabile) questi pacchetti broadcast possono accedervi. Questo è un vantaggio in reti aziendali dato che subito dopo l'avvio del computer si *vedono* tutte le stampanti disponibili, senza dover porre mano alla configurazione. Questa opzione diventa pericolosa se il computer è collegato ad Internet. Quando si configura la funzione broadcast si deve assicurare che il broadcast raggiunga solo la rete locale, che l'accesso sia consentito solo dalla rete locale e che l'indirizzo IP pubblico per il collegamento ad Internet non sia incluso nell'area di indirizzi della rete locale. Altrimenti anche gli altri utenti dello stesso ISP (Internet Service Provider) potrebbero *vedere* e utilizzare le stampanti indicate. Inoltre i broadcast generano traffico di rete, cosa che può comportare costi aggiuntivi . Dunque, in ogni caso va assicurato che i pacchetti broadcast non vengano inviati dalla stampante locale su Internet, ad esempio configurando il SuSE-Firewall per il filtraggio

dei pacchetti (`SuSEfirewall2`). Per la ricezione dei pacchetti broadcast non si deve configurare in aggiunta alcunché. Solo all'invio si deve indicare l'indirizzo broadcast (da configurare ad esempio tramite YaST2).

IPP viene utilizzato per la comunicazione tra demoni CUPS locali e remoti (dunque un *server CUPS*). Le moderni stampanti di rete supportano adesso anche *l'IPP*. Ulteriori informazioni si trovano sulle pagine Web della casa produttrice o nel manuale delle stampante. Windows 2000 e versioni successive offrono anche il supporto IPP. Purtroppo vi sono state delle difficoltà con il formato di implementazione di Windows. Probabilmente questi problemi sono stati risolti o possono essere eliminati con il service pack.

5.5.3 Configurazione del server CUPS

Vi sono tanti modi per configurare le stampanti sotto CUPS e di configurare il demone: con tool a riga di comando, YaST2, Centro di controllo di KDE, interfaccia Web etc. Nei paragrafi che seguono verranno trattati solo i tool a riga di comando e YaST2. Comunque, ripetiamo che queste non sono le uniche possibilità a vostra disposizione.

Attenzione

L'interfaccia Web comporta il rischio di compromettere la password di root, poiché la password di root viene trasmessa in forma non cifrata se nell'URL viene immesso il nome del computer. Per tale ragione si consiglia assolutamente di usare solo `http://localhost:631/` e nessun altro indirizzo.

Attenzione

Ed è anche per questo motivo che l'accesso al demone CUPS ai fini dell'amministrazione è stato ristretto in modo che potrà essere configurato solo se indirizzato con localhost (ovvero l'indirizzo IP `127.0.0.1`.) Altrimenti apparirà un messaggio di errore.

Per amministrare stampanti locali è necessario che sul computer locale giri un demone CUPS. A tal fine vanno installati il `cups` e i file PPD SuSE nei pacchetti `cups-drivers` e `cups-drivers-stp`. Quindi si inizializza il server (come `root`) con il comando: `/etc/rc.d/cups restart`. Nella configurazione YaST2 l'installazione e l'avvio avviene implicitamente selezionando CUPS come sistema di stampa e l'installazione di una stampante.

PPD sta per PostScript Printer Description ed è uno standard per descrivere opzioni della stampante tramite comandi PostScript che servono a CUPS

per l'installazione della stampante. SUSE LINUX fornisce file PPD per una vasta serie di stampanti. Comunque anche i produttori offrono sui loro siti web e CD di installazione file PPD per stampanti PostScript (spesso nella sezione Installazione sotto Windows NT).

Il demone locale può essere inizializzato per avere a disposizione localmente tutte le stampanti di tutti i server broadcast, senza disporre localmente di una sola stampante, cioé per selezionare la stampante sotto KDE e OpenOffice nel modo meno laborioso possibile.

Il broadcast si configura con YaST2, o nel file `/etc/cups/cupsd.conf` si può impostare la variabile Browsing su `On` (default) e la variabile BrowseAddress su un valore adatto (per esempio `192.168.255.255`).
Per la ricezione degli incarichi di stampa, dovete almeno premettere a `<Location /printers>`, o meglio a `<Location />` di prenderli in consegna. Dovete completare a riguardo `Allow From xyz-host.mydomain` – vedi `file:/usr/share/doc/packages/cups/sam.html`. Con il comando `/etc/rc.d/cups reload` (come `root`) viene applicata, dopo aver editato il file del demone, la nuova configurazione.

5.5.4 Stampante di rete

Una stampante di rete è una stampante con un'interfaccia di rete per il server di stampa (come è il caso per alcuni stampanti di casa HP che offrono la cosiddetta JetDirect Interface) o stampanti collegate ad un cosiddetto printserver box o router box con funzionalità di server di stampa. Non si intendono in questo contesto computer Windows che mettono la stampante a disposizione sotto forma di share, ovvero risorsa condivisa. Comunque sotto CUPS anche questo tipo di stampante è facilmente indirizzabile in modo simile.

Stampanti di rete supportano nella maggior parte dei casi il protocollo LPD (su porta `515`). Potete controllarlo con il seguente comando:

```
netcat -z
<nome host>.<dominio>
515 && echo ok || echo failed
```

Allora si possono configurare con l'URI del dispositivo (gergo CUPS) `lpd://Server/Queue`. Per ulteriori dettagli a riguardo `file:/usr/share/doc/packages/cups/sam.html`.

Solitamente è preferibile indirizzare questo tipo di stampanti tramite la porta integrata `9100` (HP, Kyocera, etc.) o la porta `35` (QMS) ad esempio senza protocollo LPD frapposto.L'URI del dispositivo sarà:

```
socket://Server:Port/
```

Per stampare con stampanti Windows deve essere installato il `samba-client` e Samba deve essere configurato in modo corretto, i. e. deve essere impostato il giusto workgroup, etc. Esistono diversi tipi di URI del dispositivo per computer che girano su Windows. Spesso comunque sarà: `smb://user:password@host/printer`. Per tutte le altre possibilità vedi `file:/usr/share/doc/packages/cups/sam.html` e "smbspool".

Dopo aver configurato la stampante di rete e si ha una piccola rete composta da diversi PC (Linux), sarebbe comodo non dover configurare la stampante di rete su ogni client. Così va attivata la funzionalità Broadcast del demone (vd. sopra.). Non è necessario neanche modificare la configurazione, p.es. dimensione standard dei fogli su `Letter` su ogni singolo client, basta farlo una volta sul server (vd. sezione 5.7.1 a pagina 119). Questi interventi vengono salvati localmente, però vengono applicati anche agli client grazie ai tool CUPS, o meglio grazie al protocollo IPP.

5.5.5 Elaborazione interna dell'incarico

Conversione verso PostScript

In linea di massima ogni tipo di file può essere inviato ad un demone CUPS. I file PostScript comunque in questo caso non creano alcuna difficoltà. La conversione in PostScript attraverso CUPS avviene dopo che il tipo di file è stato identificato sulla base di `/etc/cups/mime.types` e invocato il tool indicato in `/etc/cups/mime.convs`. Il processo di conversione avviene sul server e non sul client. Lo scopo era quello di fare in modo che la conversione si eseguisse solo sul server preposto alla stampante.

Conteggio

Dopo la conversione in PostScript, viene determinato il numero di pagine dell'incarico da stampare. A tal fine CUPS lancia il (proprio) tool pstops (`/usr/lib/cups/filter/pstops`). Il numero di pagine dell'incarico viene scritto successivamente su `/var/log/cups/page_log`. Le registrazioni sono:

- Nome della stampante (ad esempio `lp`),
- Nome dell'utente (ad esempio`root`),

- Numero dell'incarico
- Indicazione della data in parentesi quadre [],
- Il numero progressivo della pagina in fase di stampa
- Numero delle copie.

Ulteriori filtri di conversione

Inoltre potete attivare altri filtri, previa selezione delle corrispondenti opzioni di stampa. Di particolare interesse sono i seguenti:

psselect per stampare solo determinate pagine del documento,

ps-n-up per stampare più pagine del documento su un foglio.

Questi filtri non possono essere configurati. In `file:/usr/share/doc/packages/cups/sum.html` viene descritto come abilitare queste opzioni.

Conversione specifica per la stampante

Adesso avviamo il filtro necessario per generare i dati specifici da stampare. Questi filtri si trovano sotto `/usr/lib/cups/filter/`. Quale filtro sia quello giusto viene stabilito nel file PPD alla voce `*cupsFilter`, altrimenti si parte dal presupposto che si dispone di una stampante PostScript. Tutte le opzioni che dipendono dal dispositivo, come la risoluzione e la dimensione dei fogli, vengono elaborate in questo filtro.

Non è cosa da poco scrivere propri filtri per stamparti; cfr. l'articolo relativo nella banca dati di supporto *Using Your Own Filters to Print with CUPS* (Parole chiave: cups + filter).

Emissione al dispositivo di stampa

Infine viene lanciato il back-end. Si tratta di un filtro speciale che emette i dati da stampare servendosi di un dispositivo o una stampante di rete (vd. `/usr/share/doc/packages/cups/overview.html`). Il back-end consente di comunicare con il dispositivo o la stampante di rete (dipende dall'URI del dispositivo indicato durante l'installazione). Un back-end può essere per esempio `usb`, in questo caso verrebbe lanciato il programma `/usr/lib/cups/backend/usb`. Il dispositivo USB verrebbe aperto (e bloccato) e pre-inizializzato nel file system, ed i dati provenienti dal filtro verrebbero inoltrati. Alla fine, il dispositivo viene inizializzato e messo a disposizione nel sistema.

Attualmente esistono i backend:`parallelo`, `seriale`, `usb`, `ipp`, `lpd`, `http`, `socket` (dal pacchetto CUPS), nonché `canon` ed `epson` (da `cups-drivers-stp`) e `smb` (da `samba-client`).

Senza filtro

Se si vuole stampare senza alcun filtro si può immettere l'opzione `-l` per il comando `lpr`, oppure `-oraw` per `lp`. Di solito le stampanti non funzionerranno, poiché i dati non vengono convertiti (vedi sopra) o non entrano in gioco altri filtri importanti. Nel caso di altri tool di CUPS le opzioni sono simili.

5.5.6 Consigli & Trucchetti

OpenOffice

Se stampate in OpenOffice con CUPS, non dovete più, come era il caso per StarOffice 5.2, configurare le stampanti una ad una. OpenOffice le riconosce se è in esecuzione un demone CUPS a cui chiede quali sono le stampanti e le opzioni esistenti. In futuro non dovrebbe essere più necessario configurare ulteriormente OpenOffice.

Windows

Le stampanti collegate ad un computer Windows possono essere indirizzate tramite l'URI del dispositivo `smb://server/printer` – vedi sopra. Nel caso inverso, se si vuole stampare con Windows servendosi di un server CUPS, nel file di configurazione di Samba `/etc/samba/smb.conf` devono essere impostate le registrazioni `printing = CUPS` e `printicap name = CUPS` come preimpostato in SUSE LINUX.Dopo aver apportato delle modifiche in `/etc/samba/smb.conf` si deve riavviare il server Samba – vedi anche `file:/usr/share/doc/packages/cups/sam.html`

Configurare una stampante grezza (raw)

Si può configurare una stampante raw ovvero grezza ommettendo il file PPD durante l'installazione, cioé non vi sarà nè filtraggio nè conteggio. Per consentire questo i dati devono essere inviati alla stampante già nel formato compreso dalla stampante.

Opzioni della stampante propri

Le opzioni di configurazione (p.es. di solito un'altra risoluzione) possono essere modificate e salvate per ogni utenti. Le modifiche vengono memorizzate nel file `~/.lpoptions`. Se una stampante riconfigurata viene rimossa sul server, rimane visibile nei diversi tool, come `kprinter` o `xpp`. Anche se non esiste più, può essere selezionata, cosa che chiaramente comporta dei problemi. Gli utenti più esperti cancellaranno semplicemente le righe imputate da `~/.lpoptions` servendosi di un editor. Si veda a riguardo l'articolo nella nostra banca dati di supporto *Print Settings with CUPS* nonché la sezione 5.7.1 a pagina 119.

Compatibilità con LPR

CUPS può anche ricevere incarichi da sistemi LPR. Le impostazioni necessarie in `/etc/xinetd.d/cups-lpd` possono essere eseguite con YaST2, oppure manualmente.

Il debug in CUPS

Nel file di configurazione `/etc/cups/cupsd.conf` troverete la seguente sezione:

```
# LogLevel: controls the number of messages logged to the ErrorLog file
#     and can be one of the following:
#
#     debug2    Log everything.
#     debug     Log almost everything.
#     info      Log all requests and state changes.
#     warn      Log errors and warnings.
#     error     Log only errors.
#     none        Log nothing.
#
LogLevel info
```

Per l'individuazione degli errori in CUPS si imposta il `LogLevel debug` e cupsd controllerà i file di configurazione dopo aver immesso `rccups restart`. Troverete messaggi dettagliati in `/var/log/cups/error_log` che vi aiuteranno ad individuare la causa di eventuali difficoltà.

Con il seguente comando potete emettere una label o etichetta prima di eseguire un test:

```
echo "LABEL $(date)"| tee -a /var/log/cups/error_log
```

Tale etichetta verrà registrata proprio in questa forma in `/var/log/cups/error_log` per facilitare il ritrovamento dei messaggi in seguito al test.

5.6 Stampare dagli applicativi

Gli applicativi utilizzano code di stampa esistenti alla stregua dell' incarico di stampa dalla riga di comando. Per tale motivo per poter stampare dagli applicativi non viene configurata la stampante ma le code di stampa esistenti.

Per stampare dalla riga di comando si immette il comando `lp -d color` ⟨*nome_file*⟩, laddove ⟨*nome_file*⟩ va sostituito con il nome del file da stampare. Tramite l'opzione `-d` potete determinare esplicitamente la coda di stampa. Con `-d color` ad esempio viene utilizzata la coda di stampa `color`.

Il pacchetto `cups-client` include dei tool per la riga di comando relativi al processo di stampa con CUPS come il comando `lp`, in modo che quanto detto prima valga anche per CUPS (vedi la sezione 5.7). La maschera per il processo di stampa dei programmi di KDE va impostato su 'Stampa tramite programma esterno', altrimenti non si potrà eseguire alcun comando di stampa; vedi la sezione 5.8.2 a pagina 123.

Vi sono inoltre dei dialoghi grafici per la configurazione della stampa, come ad esempio xpp oppure il programma KDE kprinter che consentono non solo di selezionare la coda di stampa, ma anche di impostare opzioni di default di CUPS e di stampa del file PPD tramite menu di selezione grafici. Per avere un dialogo di stampa di kprinter uniforme nei diversi applicativi, immettete nella maschera di stampa degli applicativi come comando di stampa `kprinter` o `kprinter --stdin`. Dipende dall'applicativo quale comando utilizzare. Apparirà dopo la maschera di stampa dell'applicativo il dialogo di stampa di kprinter dove impostare la coda di stampa e le altre opzioni. Seguendo questo approccio dovete tenere presente che le impostazioni nella maschera di stampa dell'applicativo e quelle di kprinter devono essere compatibili. Consigliamo di eseguire delle impostazioni solo in kprinter!

5.7 Tool della riga di comando per il sistema di stampa CUPS

I tool della riga di comando e le relative pagine di manuale per il sistema di stampa CUPS si trovano nel pacchetto `cups-client` e la documentazione è reperibile nel pacchetto `cups` sotto `/usr/share/doc/`

packages/cups/ in particolar modo il CUPS Software Users Manual sotto file:/usr/share/doc/packages/cups/sum.html e il CUPS Software Administrators Manual sotto file:/usr/share/doc/packages/cups/sam.html che con cupsd in esecuzione localmente si trova anche sotto http://localhost:631/documentation.html.

Nel caso dei tool della riga comando CUPS a volte è determinante l'ordine delle opzioni. In caso di dubbi consultate la relativa pagina di manuale.

5.7.1 Per code di stampa locali

Generare incarichi di stampa

Di solito su System V si stampa con lp -d <coda_di_stampa> <file> e su Berkeley con lpr -P <coda_di_stampa> ⟨*file*⟩ .

Ulteriori informazioni sono reperibili nella lpr e nella lp nonché nella sezione Using the Printing System sotto file:/usr/share/doc/packages/cups/sum.html#USING_SYSTEM nel *CUPS Software Users Manual*.

Con il parametro addizionale -o possono essere stabilite opzioni di ampia portata relative al tipo di stampa. Ulteriori informazioni nella lpr e nella lp nonchè nella sezione Standard Printer Options sotto file:/usr/share/doc/packages/cups/sum.html#STANDARD_OPTIONS nel *CUPS Software Users Manual*.

Visualizzare lo stato

Lo stato di una coda di stampa viene visualizzato in System V con lpstat -o ⟨*coda di stampa*⟩ -p ⟨*coda di stampa*⟩ o in Berkeley con lpq -P⟨*coda di stampa*⟩.

Senza l'indicazione di una coda di stampa, verranno indicate tutte le code, laddove lpstat -o mostra tutti gli incarichi attivi sotto forma di ⟨*coda di stampa*⟩-⟨*numero dell'incarico*⟩.

Con lpstat -l -o⟨*coda di stampa*⟩ -p ⟨*coda di stampa*⟩ vengono mostrate più informazioni e con lpstat -t oppure lpstat -l -t viene indicato il massimo in termini di informazione disponibile.

Ulteriori informazioni nelle pagine di manuale lpq, lpstat nella sezione Using the Printing System sotto file:/usr/share/doc/packages/cups/sum.html#USING_SYSTEM nel *CUPS Software Users Manual*.

Cancellare incarichi di stampa

In System V con `cancel` ⟨*`coda di stampa`*⟩`-`⟨*`numero dell'incarico`*⟩ oppure in Berkeley con `lprm -P`⟨*`coda di stampa`*⟩ ⟨*`numero dell'incarico`*⟩ si cancella l'incarico di stampa con il numero di incarico indicato dalla coda di stampa indicata. Ulteriori informazioni nella pagina di manuale lprm e nella cancel e nella sezione Using the Printing System sotto `file:/usr/share/doc/packages/cups/sum.html#USING_SYSTEM` nel *CUPS Software Users Manual*.

Impostazioni delle code di stampa

Nel *CUPS Software Users Manual* nella sezione Standard Printer Options sotto `file:/usr/share/doc/packages/cups/sum.html#STANDARD_OPTIONS` vengono descritte opzioni standard indipendenti dall'hardware per il tipo di stampa e nella sezione Saving Printer Options and Defaults sotto `file:/usr/share/doc/packages/cups/sum.html#SAVING_OPTIONS` viene descritto come salvare le impostazioni delle opzioni.

Le opzioni specifiche della stampante per il tipo di stampa sono stabilite nel file PPD appartenente alla corrispondente coda di stampa e vengono indicate con il comando `lpoptions -p` ⟨*`coda di stampa`*⟩ `-l` nella forma seguente:

```
Option/Text: valore valore valore ...
```

laddove * caratterizza il valore dell' opzione della impostazione attuale. Esempio:

```
PageSize/Page Size: A3 *A4 A5 Legal Letter
Resolution/Resolution:150 *300 600
```

In questo caso l'opzione `PageSize` è impostata su `A4` e la risoluzione sul valore `300`.

Con `lpoptions -p` ⟨*`coda di stampa`*⟩ `-o option=valore` potete impostare un valore diverso.

In tal modo nell'esempio riportato la dimensione della carta può essere impostata su `Letter` per la relativa coda di stampa avvalendosi del seguente comando:

```
lpoptions -p <coda di stampa> -o PageSize=Letter
```

Se un utente normale, quindi non root, immette il comando `lpoptions` le impostazioni vengono salvate solo per questo utente nel file `~/.lpoptions`.

Se l'amministratore di sistema `root` immette il comando `lpoptions`, le impostazioni vengono salvati nel file `/etc/cups/lpoptions` come impostazione di default per tutti gli utenti sul computer locale. Il file PPD non viene modificato.

Solo se si modificano le impostazioni di default nel file PPD di una coda di stampa, esse saranno valide per tutti gli utenti nella rete che si servono di questa coda di stampa per stampare. L'amministratore del sistema può modificare le impostazioni di default nel file PPD di una coda di stampa in modo che nell'esempio di cui sopra la dimensione del foglio di default venga impostata per tutti gli utenti sulla rete su `Letter` per la relativa coda di stampa:

```
lpadmin -p <coda di stampa> -o PageSize=Letter
```

Vedi anche anche l'articolo della banca dati di supporto *Printing settings with CUPS*.

5.7.2 Code di stampa nella rete

⟨*Server di stampa*⟩ va sostituito con il nome o l'indirizzo IP del server di stampa e ⟨*coda di stampa*⟩ dovrà essere una coda di stampa sul server di stampa.

Qui vengono indicati solo i comandi principali. Per quanto riguarda ulteriori possibilità e fonti di informazioni vedi la sezione 5.7.1 a pagina 118.

Generare incarichi di stampa

Su System V un incarico di stampa per la coda di stampa indicata sul server di stampa indicato si genera con `lp -d` ⟨*`coda di stampa`*⟩ `-h` ⟨*`server di stampa`*⟩ ⟨*`file`*⟩ premesso che il server di stampa sia stato configurato in modo che sia consentito stampare sulle sue code di stampa. Di default questo non è dato con CUPS, ma nel modulo Configurazione della stampante di YaST2 in un ramo esteso del menu delle impostazioni per il server di CUPS ciò può essere configurato nel modo desiderato.

Visualizzare lo stato

Su System V si immette `lpstat -h` ⟨*`server di stampa`*⟩ `-o` ⟨*`coda di stampa`*⟩ `-p` ⟨*`coda di stampa`*⟩ per visualizzare lo stato di una coda di stampa sul server di stampa.

Cancellare incarichi di stampa

In System V con il comando `cancel -h` ⟨*`server di stampa`*⟩ ⟨*`coda di stampa`*⟩`-`⟨*`numero dell'incarico`*⟩ si cancella un incarico di stampa con il numero di incarico indicato dalla coda di stampa sul server di stampa.

5.7.3 Eliminare disfunzioni in CUPS con i comandi di cui sopra

Gli incarichi di stampa permangono nella coda di stampa se spegnete il computer durante il processo di stampa e riavviate Linux; un eventuale incarico di stampa con degli errori si rimuove dalla coda di stampa con il comando sopra descritto.

Se insorgono dei problemi nella trasmissione di dati tra computer e stampante, la stampante non sa cosa fare coi dati inviati e stampa innumerevoli fogli pieni di caratteri senza senso.

1. Nel caso di stampanti a getto di inchiostro rimuovete la carta o con stampanti laser aprite il cassetto della carta per interrompere il processo di stampa.
2. Dato che l'incarico di stampa viene rimosso dalla coda di stampa solo dopo che l'incarico sia stato inviato completamente alla stampante, spesso lo ritroverete nella coda di stampa. Con `lpstat -o` (o con `lpstat -h` ⟨*`server di stampa`*⟩`-o`) controllate da quale coda di stampa si sta stampando e con `cancel` ⟨*`coda di stampa`*⟩`-`⟨*`numero dell'incarico`*⟩ (o con `cancel -h` ⟨*`server di stampa`*⟩`-`⟨*`coda di stampa`*⟩`-`⟨*`numero dell'incarico`*⟩) potete cancellare l'incarico.
3. Eventualmente utilizzate il comando `fuser`.
4. Può accadere che vengano trasmessi alla stampante ancora un serie di dati nonostante che l'incarico di stampa sia stato cancellato dalla coda di stampa. Con il comando `fuser -k /dev/lp0` nel caso

di una stampante collegata alla porta parallela oppure `fuser -k /dev/usb/lp0` per una stampante USB possono essere terminati tutti i processi che accedono sulla stampante.

5. Resettate la stampante staccando per un pò la spina, riempite il cassetto della carta e riaccendete la stampante.

Se è impossibile trasmettere i dati alla stampante o il processo di trasmissione non avviene in modo corretto (p. es. viene interrotto per lungo tempo) si chiude il cosiddetto CUPS-backend preposto alla trasmissione di dati indirizzati alla stampante con un messaggio di errore (error code). L'esatta ragione del perché ciò avviene dipende dal relativo backend (p.es. backend per la porta parallela, per USB, per il server LPD, per il server IPP o per la trasmissione dei dati diretta tramite socket TCP). In questi casi il CUPS server (cupsd) disabilita il processo di stampa tramite le code interessate e le code di stampa vengono visualizzate come *disabled* o *stopped*. Dopo aver eliminato la causa del disturbo l'amministratore del sistema deve riabilitare il processo di stampa eseguendo il comando `/usr/bin/enable` ⟨*coda di stampa*⟩ (o `/usr/bin/enable -h` ⟨*server di stampa*⟩ ⟨*coda di stampa*⟩).

5.8 Stampare in una rete TCP/IP

Per informazioni dettagliate sullo spooler di stampante LPRng consultate il *LPRng-Howto* che trovate sotto `file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html`. Per CUPS vedi anche il *CUPS Software Administrators Manual* che trovate sotto `file:/usr/share/doc/packages/cups/sam.html`

5.8.1 Nomenclatura

Server di stampa Di seguito indicheremo con *server di stampa* un sistema completo dotato di sufficiente potenza di calcolo e spazio di di memoria.

Printserver box e stampanti di rete

- Il printserver box è un piccolo dispositivo con una connessione di rete TCP/IP da una parte nonché la possibilità di connessione

locale per una stampante. Vi sono anche *box di router* che dispongono di una possibilità di connessione per una stampante e che vanno trattati alla stregua di printserver box.

- Una stampante di rete dispone di una propria connessione di rete TCP/IP. In fin dei conti si tratta di una stampante con un printserver box integrato. Stampanti di rete e printserver box vanno dunque trattati allo stesso modo.

Sussiste una grande differenza tra una stampante di rete o printserver box da una parte e un server di stampante vero e proprio dall'altra. Vi sono anche grandi stampanti che forniscono a corredo un computer completo come server di stampa di rete. Ma in questi casi, per stampare viene indirizzato il server di stampa fornito a corredo, e non la stampante.

Server LPD Un *server LPD* è un server di stampa indirizzabile tramite il protocollo LPD. Questo caso si ha quando sul server di stampa gira il sistema di stampa *LPRng/lpdfilter* (per la precisione l' lpd) oppure se il sistema di stampa *CUPS* è in esecuzione ed è stato configurato in modo che la macchina risulti indirizzabile anche tramite il protocollo LPD (per la precisione il cups-lpd).

Server IPP e server CUPS Un server IPP oppure un server CUPS sono dei server di stampa indirizzabili tramite il rotocollo IPP, il che è il caso se sul server di stampa è in esecuzione il sistema di stampa CUPS o più precisamente il cupsd.

Server di rete CUPS Come *server di rete CUPS* intendiamo un *server CUPS* configurato in modo che comunica le proprie code di stampa agli altri host sulla rete per UDP broadcast (tramite la porta UDP `631`).

5.8.2 Configurazione rapida di un client

Sulla rete un client di solito non dispone di una stampante collegata localmente, gli incarichi di stampa vengono inviati dal client al server di stampa. Se si dispone un server di stampa e al client è connessa un'ulteriore stampante dovete configurare oltre al client anche la stampante collegata in locale. Scegliete un sistema di stampa sul client consono a quello del server.

Configurazione client per un server LPD

Se nella rete non vi è alcun server di rete CUPS ma solo un server LPD, si consiglia di utilizzare sul cliente il sistema di stampa `LPRng/lpdfilter`.

In tal modo non si rende necessario configurare ulteriormente il client dal momento che lo spooler LPRng riesce ad indirizzare direttamente anche code di stampa remote con il comando lpr.

La premessa è che il server LPD sia stato configurato in modo che il client possa servirsi sue delle code di stampa. Per stampare da applicativi si immette nell'applicativo il comando `lpr -P⟨coda di stampa⟩@⟨ server di stampa⟩` .

Alcuni applicativi sono preimpostati su CUPS e vanno perciò impostati su LPRng. In particolar modo KDE ed il programma di stampa di KDE kprinter devono essere impostati su 'Stampa tramite programma esterno', perché altrimenti non funziona il comando di stampa riportato sopra.

Configurazione client per un server di rete CUPS

Se il server di stampa è un server di rete CUPS allora con la configurazione della stampante di YaST2 -premendo prima su 'Modifica' ed in seguito su 'Esperti...' - potrete scegliere tra le seguenti possibilità:

CUPS quale server (di default nell'installazione standard)
Se non è collegata alcuna stampante in locale non è stata neanche configurata alcuna coda di stampa con YaST2. In questo caso cupsd non viene lanciato automaticamente. Per lanciare cupsd bisogna attivare il servizio 'cups' (di solito per i runlevel 3 e 5)

Non bisogna intervenire sul client, poiché il server di rete CUPS comunica ad intervalli regolari via broadcast a tutti gli host sulla rete le proprie code di stampa in modo che dopo un breve periodo di attesa sul client sono disponibili le code di stampa del server di rete CUPS.

La premessa è che il server di rete CUPS sia configurato in modo che la funzionalità di broadcast sia abilitata e che venga utilizzato un indirizzo broadcast adatto al client e che il client abbia il permesso di servirsi delle code di stampa del server di rete CUPS per stampare.

CUPS esclusivamente come client Se si vuole stampare tramite le code di stampa del server di rete CUPS basta che CUPS giri solo come client; in YaST2 bisogna a riguardo attivare solo la voce *Client-only* nella maschera di configurazione della stampante e indicare il nome del server di rete CUPS.

In questo caso sul client non gira alcun cupsd e dunque non vi è neanche alcun file `/etc/printcap`. Gli applicativi che non possono essere impostati su CUPS offrono però solo code di stampa che sono riportate nel file locale `/etc/printcap`. In questi casi si consiglia di

far girare CUPS come server in modo che venga creato automaticamente dal cupsd locale un file `/etc/printcap` con i nomi delle code di stampa del server di rete CUPS.

5.8.3 Protocolli di stampa in una rete TCP/IP

Vi sono le seguenti possibilità per stampare in una rete TCP/IP che si distinguono non tanto per quanto riguarda l'hardware impiegato, ma per il protocollo utilizzato. Per tale ragione durante la configurazione della stampante con YaST2 si distingue in base al protocollo e non in base all'hardware.

Nonostante ciò, nella procedura di configurazione della stampante di YaST2 viene innanzitutto selezionato tramite quale tipo di "hardware" debba realizzarsi il processo di stampa (ad esempio tramite server di rete CUPS, server di rete LPD o stampa diretta tramite una stampante di rete o printserver box). Quindi si potrà scegliere solamente tra i protocolli possibili, laddove è preselezionato il protocollo che dovrebbe funzionare per la maggioranza dei casi; se è ammesso solo un protocollo, non vi è possibilità di scelta. Esempi:

- Stampare tramite server di rete CUPS
  - Protocollo IPP (unica possibilità)
- Stampare tramite server di rete LPD
  - Protocollo LPD (unica possibilità)
- Stampa direttamente su stampante di rete oppure printserver box:
  - TCP-socket
  - Protocollo LDP
  - Protocollo IPP

Affinché i dati possano essere trasmessi dall'emittente al destinatario in base ad un determinato protocollo, il mittente ed il destinatario devono offrire il supporto per il protocollo in questione. Sia il software in esecuzione del mittente che del ricevente devono supportare il protocollo.

In fin dei conti non fa differenza quale tipo di hardware e software venga utilizzato, quello che conta è che sia il mittente che il ricevente supportino

il relativo protocollo. In base al protocollo vengono trasmessi incarichi di stampa o solo dati grezzi.

Un incarico di stampa contiene oltre ai dati da stampare anche informazioni aggiuntive — ad esempio quale utente su quale sistema ha generato l'incarico di stampa ed eventualmente le relative opzioni di stampa specificati (p. e. dimensione dei fogli e/o se debba venir eseguita una stampa duplex, etc.)

Stampare tramite il protocollo LPD

L'incarico di stampa viene inviato tramite il protocollo LPD ad una coda di stampa del destinatario. Secondo il protocollo LPD il destinatario riceve gli incarichi di stampa sulla porta 515, dunque è richiesto un servizio che prenda in consegna gli incarichi sulla porta 515 (di solito si tratta del servizio lpd) ed inoltre serve una coda di stampa che memorizza temporaneamente gli incarichi di stampa.

Mittenti che supportano il protocollo LPD:

Computer Linux con sistema di stampa LPRng:

- LPRng supporta l'invio di incarichi tramite il protocollo LPD attraverso l' lpd. Serve una coda di stampa sul sistema mittente dalla quale l'lpd del mittente prende l'incarico di stampa e lo inoltra all' lpd del destinatario.
- Nel caso di LPRng ciò funziona anche senza lpd locale. Il programma lpr del pacchetto lprng inoltra l'incarico di stampa tramite il protocollo LPD direttamente all'lpd del destinatario.

Computer Linux con sistema di stampa CUPS-server:

- CUPS supporta l'invio degli incarichi tramite il demone CUPS (cupsd). Serve una coda di stampa sul sistema mittente da cui cupsd prende l'incarico di stampa ed lo invia all'lpd del destinatario.

Computer Linux con sistema di stampa CUPS-client:

- L'invio tramite il protocollo LPD nel sistema di stampa CUPS-client non viene supportato.

Computer con sistema operativo di terzi:

- Il protocollo LPD non è proprio recente, quindi ogni sistema operativo dovrebbe supportare questo protocollo almeno come mittente. Eventualmente il supporto non è attivato di default, allora bisognerà installare del software appropriato.

Mittenti che supportano il protocollo LPD:

Computer Linux con sistema di stampa LPRng:

- LPRng supporta la ricezione tramite il protocollo LPD attraverso l'lpd.

Computer Linux con sistema di stampa CUPS-server:

- CUPS supporta la ricezione tramite il protocollo LPD attraverso il cups-lpd. Il cups-lpd si attiva tramite inetd o xinetd.

Computer Linux con sistema di stampa CUPS-client:

- La ricezione tramite il protocollo LPD non viene supportata con il sistema di stampa CUPS-client.

Server di stampa e printserver box/ stampante di rete:

- Il protocollo LPD non è proprio recente, quindi ogni normale server di stampa e normale printserver box o stampante di rete dovrebbe supportare questo protocollo.
- Nel caso di printserver box o stampanti di rete il nome della coda di stampa varia da modello a modello o vi sono diverse code di stampa che si distinguono nel loro comportamento.

Stampare tramite il protocollo IPP

Il mittente invia un incarico di stampa tramite il protocollo IPP ad una coda di stampa del ricevente. Il destinatario riceve gli incarichi di stampa in base al protocollo IPP sulla porta 631. Anche sul sistema ricevente quindi è necessario un servizio che accetti gli incarichi sulla porta 631(nel caso di CUPS si tratta di cupsd) ed inoltre una coda di stampa in cui memorizzare temporaneamente gli incarichi di stampa accettati.

Mittenti che supportano il protocollo IPP:

Computer Linux con sistema di stampa LPRng:

- LPRng non supporta il protocollo IPP.

Computer Linux con server CUPS o sistema di stampa CUPS-client:

- CUPS supporta l'invio degli incarichi tramite il protocollo IPP anche senza cupsd locale. I programmi lpr o lp dal pacchetto cups-client oppure il programma xpp o il programma KDE kprinter gli incarichi di stampa possono inoltrare direttamente al destinatario gli incarichi di stampa tramite il protocollo IPP.

Computer con sistema operativo di terzi:

- Il protocollo IPP è relativamente recente in modo che il supporto varia da caso a caso.

Mittenti che supportano il protocollo IPP:

Computer Linux con sistema di stampa LPRng:

- LPRng non supporta il protocollo IPP.

Computer Linux con sistema di stampa CUPS-server:

- CUPS supporta la ricezione di incarichi tramite il protocollo IPP attraverso il cupsd. Serve una coda di stampa sul computer ricevente nella quale il cups-lpd possa memorizzare temporaneamente l'incarico di stampa ricevuto dal mittente.

Computer Linux con sistema di stampa CUPS-client:

- La ricezione tramite il protocollo IPP non viene supportato col sistema di stampa CUPS-client.

Server di stampa e printserver box/stampante di rete:

- Il protocollo IPP è relativamente recente in modo che il supporto dipende dal caso specifico.

Stampare direttamente tramite il socket TCP

In questo caso l'incarico della stampante non viene inviato ad una coda di stampa remota, poiché non vi è alcun protocollo (né LPD né IPP), che riesca a gestire incarichi di stampa o code di stampa. Invece i dati grezzi vengono inviati direttamente tramite un socket TCP ad una porta TCP remota, di solito ciò viene utilizzato per trasmettere i dati specifici da stampare a printserver box e stampanti di rete. In molti casi viene utilizzata la porta TCP 9100.

Mittenti che supportano la stampa direttamente tramite il socket TCP:

Computer Linux con sistema di stampa LPRng:

- LPRng supporta l'invio degli incarichi direttamente tramite il socket TCP attraverso l'lpd. Serve una coda di stampa sul computer mittente da cui l'lpd del mittente prenda l'incarico di stampa ed invii i dati da stampare alla porta TCP del destinatario.
- Con LPRng questo funziona anche senza lpd locale. Il programma lpr dal pacchetto lprng è in grado ricorrendo alla opzione `-Y` di inviare i dati da stampare direttamente via socket TCP alla porta TCP del destinatario. Vedi la pagina di manuale relativa a lpr.

Computer Linux con sistema di stampa CUPS-server:

- CUPS supporta l'invio degli incarichi direttamente tramite il socket TCP attraverso il cupsd. Serve una coda di stampa sul computer mittente dalla quale il cupsd prenda l'incarico di stampa ed invii i dati da stampare alla porta TCP del destinatario.

Computer Linux con sistema di stampa CUPS-client:

- L'invio diretto tramite il socket TCP non viene supportato col sistema di stampa CUPS-client.
- Comunque con il seguente comando è possibile inviare dei dati alla porta di un computer:

```
cat <nome file> | netcat -w 1 <host> <port>
```

Mittente che supportano la stampa direttamente tramite il socket TCP:

Computer Linux con sistema di stampa LPRng o CUPS-server o CUPS-client:

- Per ricevere dei dati direttamente tramite il socket TCP non è necessario alcun sistema di stampa e nessuno dei sistemi di stampa supporta ciò direttamente, visto che non ha senso inviare dei dati grezzi se vi è un sistema di stampa che supporti dei veri incarichi di stampa e un protocollo adatto (LPD o IPP).
- Comunque con il sistema di stampa CUPS è possibile accettare dei dati anche tramite la porta 9100 ed inoltrarli ad una coda di stampa immettendo in `/etc/inetd.conf`:
  ```
  9100 stream tcp nowait lp /usr/bin/lp lp -d <coda di stampa>
  ```
  Se non vi deve essere alcun filtraggio, va aggiunto `-o raw`.
- Inoltre è possibile emulare il comportamento di un printserver box che accetta dei dati tramite la porta 9100 e li invia direttamente alla stampante, inserendo in `/etc/inetd.conf` un rigo del tipo:
  ```
  9100 stream tcp nowait lp /bin/dd dd of=/dev/lp0
  ```

Printserver box o stampante di rete:

- Il supporto dipende dal caso specifico.
- In particolar modo la porta esatta varia da modello a modello. Nel caso di stampanti di rete HP o printserver box JetDirect si ha di default la porta 9100 o rispettivamente per i printserver box JetDirect con due o tre connessioni locali per stampanti le porte 9100, 9101 e 9102. Queste porte vengono utilizzate anche da tanti altri printserver-box. Consultate il manuale del printserver-box e in caso di dubbio rivolgetevi al produttore del printserver-box o stampante di rete per sapere tramite quale porta è possibile indirizzare direttamente la stampante. Per delle ulteriori informazioni a riguardo sono reperibili nel LPRng-Howto che trovate sotto `file:///usr/share/doc/packages/lprng/LPRng-HOWTO.html` e lì in particolar modo sotto `file:///usr/share/doc/packages/lprng/LPRng-HOWTO.html#SECNETWORK`, `file:///usr/share/doc/packages/lprng/LPRng-HOWTO.html#SOCKETAPI` e

```
file:///usr/share/doc/packages/lprng/LPRng-
HOWTO.html#AEN4858
```

Esempi

Caso 1: Diversi postazioni di lavoro, un server di stampa e uno o più printserver box o stampante di rete:

Server di stampa con sistema di stampa LPRng:

- Le postazioni di lavoro dovrebbero utilizzare anche il sistema di stampa LPRng.
- Per ogni stampante connessa ad un printserver box o per ogni stampante di rete vi è sul server di stampa un propria coda di stampa.
- Le postazioni di lavoro trasmettono gli incarichi di stampa tramite il protocollo LPD alla coda di stampa sul server di stampa appartenente alla stampante.
- A seconda del protocollo supportato dal printserver box o dalla stampante di rete, il server di stampa utilizza il protocollo LPD o trasmette i dati direttamente tramite il socket TCP per inviare i dati da stampare al printserver box o alla stampante di rete.

Server di stampa con il sistema di stampa CUPS-server:

- Le postazioni di lavoro dovrebbero utilizzare anche il sistema di stampa CUPS. In questi casi il sistema di stampa CUPS-client è del tutto sufficente.
- Per ogni stampante connessa ad un printserver box o per ogni stampante di rete vi è sul server di stampa una propria coda di stampa.
- Le postazioni di lavoro trasmettono gli incarichi di stampa tramite il protocollo IPP alla coda di stampa appartente alla stampante sul server di stampa.
- A seconda del protocollo supportato dal printserver box o dalla stampante di rete, il server di stampa utilizza il protocollo LPD o trasmette i dati direttamente tramite il socket TCP per inviare i dati da stampare al printserver box o alla stampante di rete.

Caso 2: Alcune poche postazioni di lavoro, nessun server di stampa e uno o più printserver box o stampante di rete:

Postazioni di lavoro con sistema di stampa LPRng o CUPS-server:

- Per ogni stampante connessa al printserver box o per ogni stampante di rete vi è su ogni postazione di lavoro una propria coda di stampa. Visto che su ogni postazione di lavoro devono essere configurate tutte le code di stampa, questo procedimento è sensato solo con un numero ristretto di postazioni di lavoro.
- A seconda del protocollo supportato dal printserver box o dalla stampante di rete, la postazione di lavoro utilizza il protocollo LPD o trasmette i dati direttamente tramite il socket TCP per inviare i dati da stampare al printserver box o alla stampante di rete.
- Se diverse postazioni di lavoro inviano contemporaneamente dei dati allo stesso printerserver box o stampante di rete, può verificarsi una perdita di dati e tutta una serie di problemi — soprattutto se per la trasmissione dei dati viene utilizzato il protocollo LPD, dato che spesso l'implementazione dell'LPD del destinatario sul printserver box o stampante di rete non è sufficente, perché spesso non vi è abbastanza spazio di memoria per accettare diversi incarichi di stampa e memorizzarli temporaneamente. Se invece la trasmissione dei dati avviene esclusivamente tramite il socket TCP, ciò può funzionare in modo ineccepibile a seconda del printserver box o stampante di rete.

5.8.4 Filtraggio durante il processo di stampa nella rete

Nella sezione precedente è stato descritto il modo in cui gli incarichi di stampa o i dati grezzi vengono inviati dalla postazione di lavoro alla stampante. Tutt'altro discorso vale per il filtraggio (dunque la conversione dei dati originari in dati da stampare) nel processo di stampa tramite rete. Questa conversione quando si stampa tramite rete avviene esattamente come nel caso di una stampante collegata localmente ad una postazione di lavoro singola. Per quel che riguarda il filtro di stampa non vi è alcuna differenza tra stampa tramite rete e postazione di lavoro singola. Solamente il flusso di dati da una postazione di lavoro verso la stampante è più complesso interessando diversi dispositivi, ad esempio:

```
Postazione di lavoro ->
Server di stampa ->
Printserver-box ->
Stampante
```

Proprio a questo punto della catena il file di origine deve venire convertito nel formato che la stampante riesce a stampare (PostScript, PCL, ESC/P).

La conversione viene realizzata dal filtro della stampante che può funzionare solo su un computer con sufficiente potenza di calcolo e capacità di memoria, dunque o su una postazione di lavoro o su un server di stampa, ma non in un printserver box o stampante di rete. Le stampanti di rete e printserver box di solito non hanno un filtro della stampante integrato, quindi possono accettare solo dati da stampare ed inoltrarli alla stampante o dispositivo di stampa vero e proprio.

Una coda di stampa può essere impostata con o senza filtraggio. Dato che nella configurazione della stampante in YaST2 si seleziona innazitutto tramite quale tipo di hardware debba avvenire la stampa (p.e. tramite server di rete CUPS, server di rete LPD o stampa diretta su una stampante di rete o printserver box), il valore di default consente normalmente un corretto funzionamento — altrimenti vanno adattati i valori di default nella configurazione della stampante di YaST2.

I valori di default sono:

Stampare tramite server di rete CUPS:
nessun filtraggio (dato che di solito ciò avviene sul server di rete CUPS)

Stampare tramite il server di rete LPD:
nessun filtraggio (dato che di solito ciò avviene sul server di rete LPD)

Stampa diretta su una stampante di rete o un printserver box:
Filtraggio

Impostando una coda di stampa con filtraggio, i dati originari vengono memorizzati temporaneamente nella coda di stampa. Una volta inviati i dati al destinatario, essi vengono filtrati sulla macchina sulla quale si trova la coda di stampa. Al processo di trasmissione vero e proprio viene anteposto il filtraggio, in modo che il destinatario riceva i dati convertiti (Figura 5.2 nella pagina successiva).

Segue una rassegna delle possibilità date per quel che riguarda il filtraggio negli esempi riportati sopra.

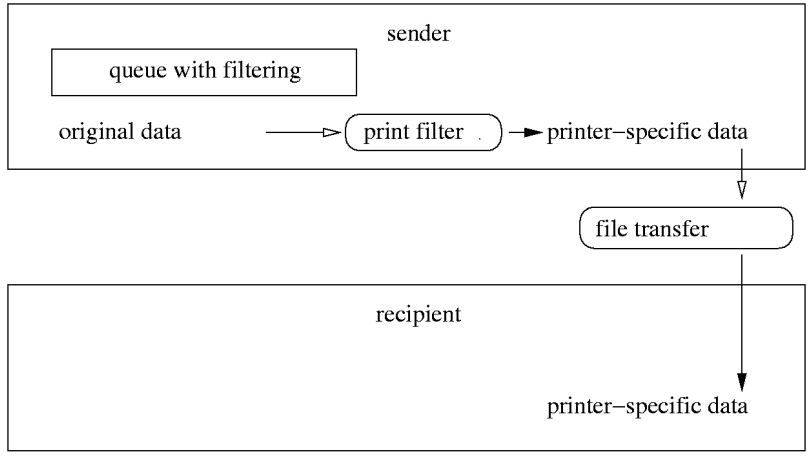

Figura 5.2: *Il processo di filtraggio*

Caso B1: Diverse postazioni di lavoro, un server di stampa e uno o più printserver box o stampante di rete: La configurazione più semplice e sensata è quella riportata nella figura 5.3 a fronte.

Caso B1b Per ogni coda di stampa con filtraggio sul server di stampa si può creare una coda di stampa configurata in modo corrispondente senza filtraggio su ogni postazione di lavoro, in modo che in caso di una disfunzione temporanea o sovraccarico del server di stampa gli incarichi di stampa possano essere memorizzati temporaneamente sulle postazioni di lavoro. Così si potrà stampare dalle postazioni di lavoro senza dover attendere che il server di stampa sia nuovamente disponibile. Lo svantaggio è che si dovranno configurare tutte le code di stampa su ogni postazione di lavoro (senza filtraggio!) e bisognerà allineare la configurazione di tutte le postazioni di lavoro in caso di modifiche delle code di stampa sul server di stampa (ad esempio se si modificano i nomi o se vengono aggiunte o rimosse code di stampa, ma non se si effettuano delle modifiche che interessano il filtraggio).Questo configurazione davvero complessa assume l'aspetto riportato nella figura 5.4 a pagina 136.

Caso B1c Teoreticamente il filtraggio potrebbe avvenire su ogni postazione di lavoro con il server di stampa che inoltrerebbe i dati da stampare solo ai printserver box o stampanti di rete; ma in tal modo si ri-

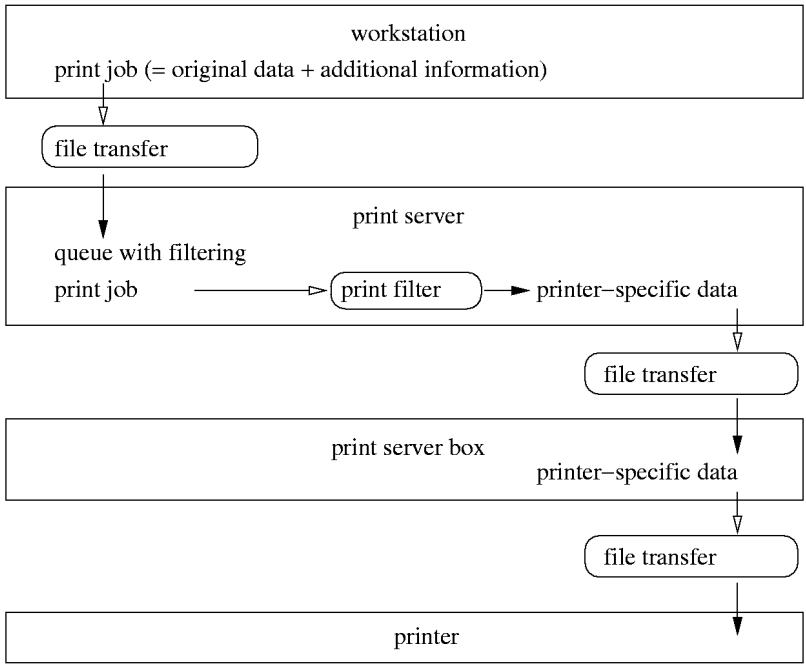

Figura 5.3: *Configurazione 1*

durebbero i server di stampa ad una specie di grossi printserver box, cosa non proprio sensata nella prassi, almenoché il server di stampa sia talmente limitato nelle sue prestazioni che il filtraggio causerebbe un sovraccarico. Lo svantaggio in questo caso sarebbe che bisognerebbe configurare tutte le code di stampa anche su ogni postazione di lavoro (con filtraggio) e che ad ogni modifica la configurazione sarebbe da allineare su tutte postazioni di lavoro.

Questo tipo di configurazione assumerebbe l'aspetto riportato nella seguente figura 5.5 a pagina 137.

Caso B2 Alcune poche postazioni di lavoro, nessun server di stampa e uno o più printserver box o stampante di rete: l'unica possibile configurazione consiste nell'impostare una coda di stampa con filtraggio per ogni stampante su ogni postazione di lavoro. Lo svantaggio è che si debbono configurare tutte le code di stampa su ogni postazione di lavoro (rispettivamente con filtraggio) e che ad ogni modifica si dovrà

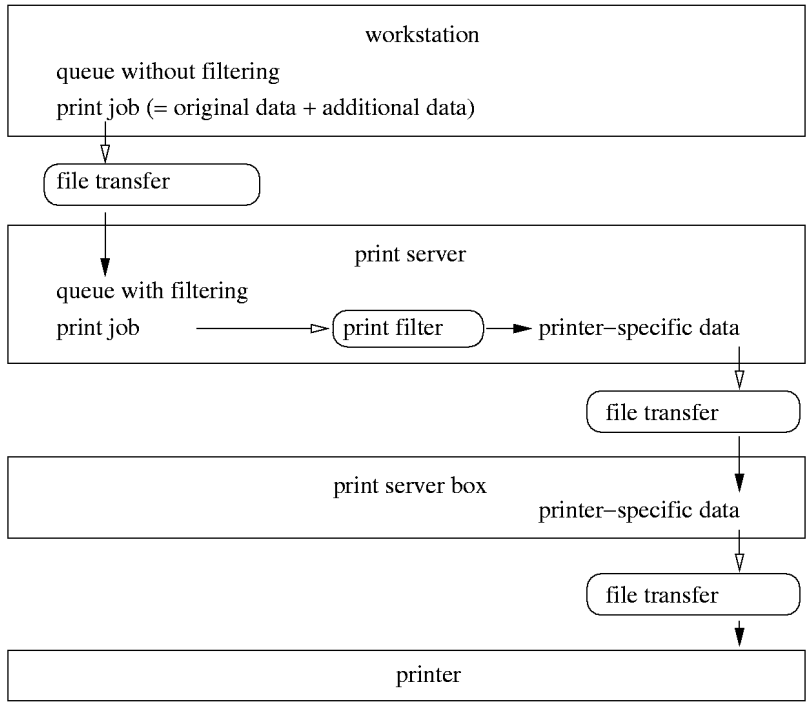

Figura 5.4: *Configurazione 2*

allineare la configurazione delle singole postazioni di lavoro. Questo tipo di configurazione viene illustrata nella figura 5.6 a pagina 138.

Caso B3 Il caso precedente è molto simile alla configurazione di una postazione di lavoro singola con stampante collegata in locale.Per un raffronto la configurazione della figura 5.7 a pagina 139 per una postazione di lavoro singola:

Se andiamo a ritroso nei casi sovramenzionati, vediamo i passaggi in tema di configurazione per una postazione di lavoro singola con stampante collegata in locale fino ad arrivare ad una complessa o meglio efficace configurazione per diverse postazioni di lavoro con un server di stampa per diversi printserver box o stampanti di rete.

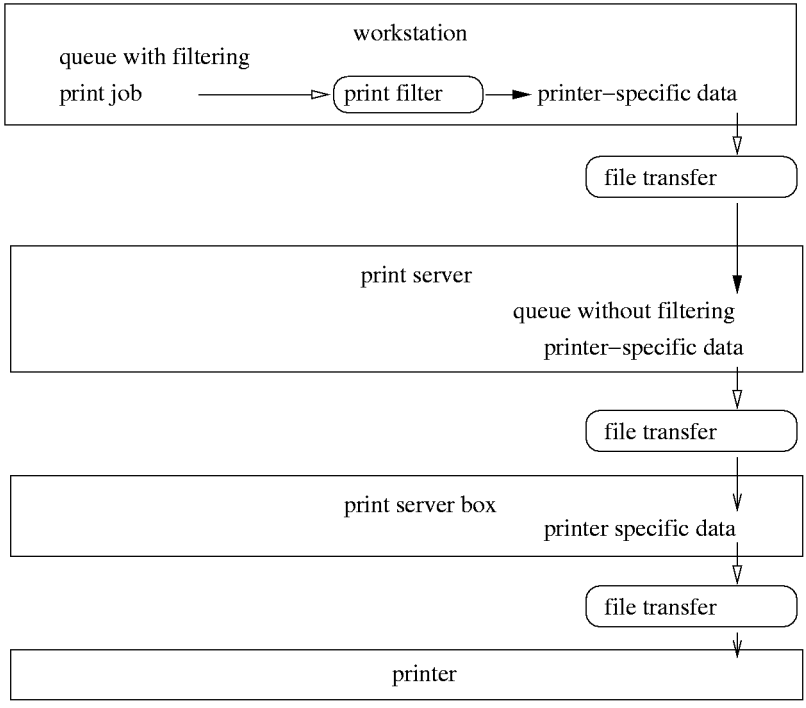

Figura 5.5: *Configurazione 3*

5.8.5 Risoluzione di problemi

Controllate la rete TCP/IP La rete TCP/IP compresa la risoluzione dei nomi devono funzionare in modo ineccepibile.

Controllate la configurazione del filtro
Collegate direttamente la stampante alla prima interfaccia parallela del computer. Configurate la stampante solo ai fini di un test come stampante locale per escludere possibili problemi dovuti alla rete. Se la stampante funziona in locale, state usando i giusti driver Ghostscript e parametri per la configurazione del filtro.

Controllate un lpd remoto Con il seguente comando potete verificare se sia possibile un collegamento TCP all'lpd (porta 515) sul computer ⟨*host*⟩:

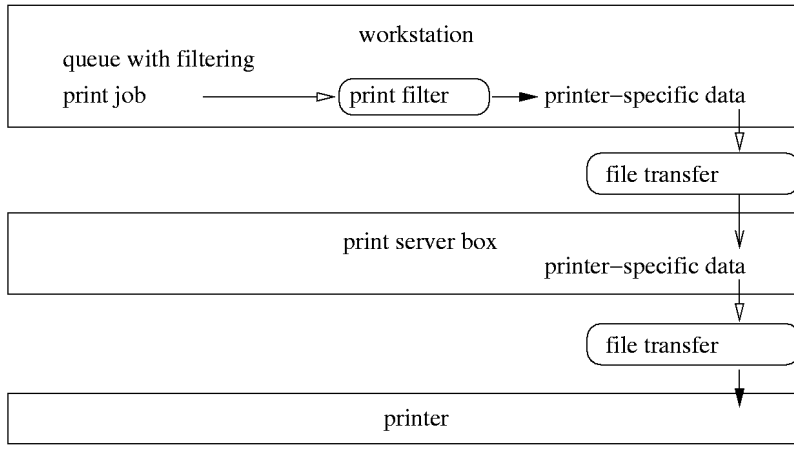

Figura 5.6: *Configurazione 4*

```
netcat -z <host> 515 && echo ok || echo failed
```

In caso negativo, il problema è dovuto o all' lpd o alla rete.

Come utente `root` si ottiene con il seguente comando un resoconto (eventualmente molto dettagliato) sulla coda di stampa ⟨*queue*⟩ sul computer remoto ⟨*host*⟩, sempre che l'lpd del computer remoto funzioni ed è possibile inviarci delle richieste.

```
echo -e "\004<queue>" \
    | netcat -w 2 -p 722 <host> 515
```

Se l'lpd non risponde, ci sono due possibilità: o non funziona l'lpd, o vi è una grave disfunzione della rete. Se ottenete una risposta dall'lpd, questa dovrebbe chiarire la ragione per la quale sulla coda di stampa `queue` del computer `host` non sia possibile stampare – esempi:

Exempio 5.1: *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
```

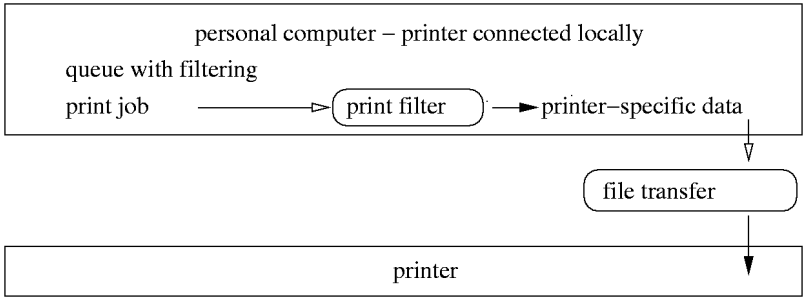

Figura 5.7: *Configurazione 5*

Nel caso di una risposta simile da parte dell'lpd, il problema è dovuto all'lpd remoto.

Controllate un cupsd remoto Con il seguente comando si può verificare se nella rete vi è un server di rete CUPS, il quale dovrebbe inviare un broadcast tramite la porta UPD `631` ogni 30 secondi comunicando le proprie code di stampa:

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

Dopo 40 secondi dovrebbe apparire un output simile a quello riportato, se vi è un server di rete CUPS che invia dei broadcast:

Exempio 5.2: *Broadcast da un server di rete CUPS*

```
... ipp://<host>.<domain>:631/printers/<queue>
```

Con il seguente comando si può testare se è possibile creare un collegamento TCP al cupsd (porta 631) sul computer ⟨*host*⟩:

```
netcat -z <host> 631 && echo ok || echo failed
```

In caso negativo, o cupsd non è in esecuzione o si ha un problema di rete.

```
lpstat -h <host> -l -t
```

fornisce un resoconto (eventualmente molto dettagliato) sulle code di stampa che si trovano sul computer⟨*host*⟩, sempre se su questo computer il cupsd sia in esecuzione e che sia possibile inviarci delle richieste.

```
echo -en "\r" \
    | lp -d <queue> -h <host>
```

permette di verificare se la coda di stampa ⟨*queue*⟩su ⟨*host*⟩ accetti un incarico di stampa, laddove l'incarico consiste di un solo carattere di ritorno di carrello, cioè si vuole eseguire solo un test senza stampare effettivamente; alla fine dovrebbe venire emesso solo un foglio bianco.

Controllate un server SMB remoto

La funzione basilare si lascia verificare con il seguente comando:

```
echo -en "\r" \
    | smbclient '/<HOST>/<SHARE>' '<PASSWORD>' \
          -c 'print -' -N -U '<USER>' \
          && echo ok || echo failed
```

Al posto di ⟨*HOST*⟩ va immesso il nome host del server Samba, al posto di ⟨*SHARE*⟩ il nome della share remota (ad esempio il nome della share Samba), al posto di ⟨*PASSWORD*⟩ la password e al posto di ⟨*USER*⟩ il nome dell'utente. In questo caso si effettua solo un test, di solito non si dovrebbe stampare alcunché e se sì allora solo un foglio bianco.

Con il seguente comando visualizzate le share disponibili su ⟨*host*⟩ — vd. la pagina di manuale smbclient:

```
smbclient -N -L <host>
```

La stampante di rete o il printserver box non funzionano ineccepibilmente

A volte si verificano dei problemi con lo spooler della stampante che gira in un printserver box, non appena c'é tanto da stampare. Visto che il problema é dovuto al printserver box, non si può fare nulla. Si può aggirare lo spooler del printserver box indirizzando direttamente la stampante collegata al printserver box tramite il socket TCP.

In questo modo il printserver box funge solamente da convertitore tra le diverse possibilità di trasmissione dei dati (rete TCP/IP e collegamento della stampante locale), così la stampante collegata al printserver box si comporta come una stampante collegata in locale. Avrete

un controllo più diretto sulla stampante, più di quanto che non con lo spooler frapposto sul printserver box. Comunque in questo caso deve essere nota la relativa porta TCP sul printserver box. Se la stampante è collegata al printserver box ed è accesa, tramite il programma `nmap` dal pacchetto `nmap`, ad printserver box acceso si lascia determinare in poco tempo la porta TCP in questione.

Ecco l'output di `nmap` nel caso di un printserver box:

```
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 significa:

- Potete entrare nel printserver box tramite `telnet`, in modo da poter ricercare informazioni basilari ed intervenire sulla configurazione.
- Tramite HTTP potete indirizzare un server web che gira in un printserver box. Esso fornisce informazioni dettagliate e permette una configurazione dettagliata.
- Tramite la porta `515` potete indirizzare per via del protocollo LPD lo spooler che gira nel printserver box.
- Attraverso la porta `631` potete indirizzare tramite il protocollo IPP lo spooler che gira nel printserver box.
- Attraverso la porta `9100` potete indirizzare tramite socket il TCP la stampante collegata al printserver box.

Di default `nmap` controlla solo una determinata lista di porte note, registrate in `/usr/share/nmap/nmap-services`. Per controllare tutte le porte immettete `nmap -p` ⟨*from_port*⟩-⟨*to_port*⟩ ⟨*IP-address*⟩ (può durare un pò) vedi a riguardo la pagina di manuale con `man nmap`.

Con comandi del tipo

```
echo -en "\rHello\r\f" | netcat -w 1 <indirizzo IP> <porta>
cat <file> | netcat -w 1 <indirizzo IP> <porta>
```

una serie di caratteri o file possono essere inviati direttamente ad una determinata porta per verificare se la stampante risulti indirizzabile tramite la porta in questione.

5.8.6 Server di stampa LPD ed IPP

LPD, IPP e CUPS

Un server CUPS supporta solitamente solo il protocollo IPP. Il programma `/usr/lib/cups/daemon/cups-lpd` dal pacchetto cups permette comunque, che un server CUPS accetti anche incarichi di stampa inviatigli alla porta 515 tramite il protocollo LPD. Dovete abilitare il relativo servizio per l'`xinetd` — solitamente con YaST2 o manualmente, attivando il rigo corrispondente nel file `/etc/xinetd.d/cups-lpd`.

LPRng/lpdfilter e CUPS

Alcuni vorranno far girare entrambi i sistema di stampa LPRng/lpdfilter e CUPS sullo stesso computer, ad esempio per aggiungere CUPS al server di stampa LPD, o perché in alcuni casi particolari si necessita il sistema di stampa LPRng/lpdfilter.

In linea di massima sorgono delle difficoltà se i due sistemi debbano coesistere su un computer. Qui verranno accennati brevemente alcuni dei problemi e le restrizioni che ne risultano. La tematica comunque è troppo complessa per poter proporre in questa sede una soluzione.

- La configurazione della stampante non dovrebbe essere eseguita con YaST2, poiché la configurazione della stampante con YaST2 non è adatta per questi casi.
- Vi è un conflitto tra i pacchetti lprng e cups-client, dato che contengono file omonimi p.e. `/usr/bin/lpr` e `/usr/bin/lp`. Quindi non va installato il pacchetto cups-client con la conseguenza che non vi sono tool di riga di comando CUPS, ma solo per LPRng. Comunque sarà possibile stampare servendosi delle code di stampa CUPS in modalità grafica con xpp o kprinter, e dagli applicativi che supportano direttamente CUPS.
- Di default cupsd al suo avvio aggiorna il file `/etc/printcap` con solo i nomi delle code di stampa CUPS per ragioni di compatibilità, poiché numerosi applicativi leggono i nomi delle code di stampa da `/etc/printcap` per poterli mettere a disposizione nel menu della stampante. Questo non deve avvenire per cupsd, in modo che `/etc/printcap` serva solo per l'uso del sistema di stampa LPRng/lpdfilter. La conseguenza è che gli applicativi che utilizzano solo code di stampa di `/etc/printcap`, mostrano solo le code di stampa locali, e non tutte le code di stampa CUPS disponibili sulla rete.

Ulteriori indicazioni sul processo di stampa

In questo capitolo facciamo luce sulle cognizioni di base riguardanti il processo di stampa. Con degli esempi alla mano vengono chiariti i nessi del funzionamento della stampante, cosa che agevolerá trovare la soluzione per particolari casi di applicazione.

6.1 Configurazione manuale di porte di stampanti locali

6.1.1 Porte parallele

Di solito una stampante si collega ad un sistema Linux attraverso una porta parallela. Una stampante collegata alla porta parallela viene indirizzata attraverso il sottosistema `parport` del kernel. La configurazione di base di una porta parallela con YaST2 viene descritta nella sezione 5.3.4 a pagina 106, di seguito riportiamo perciò degli approfondimenti:

Attraverso il caricamento di moduli del kernel di una specifica architettura si devono "comunicare" le porte parallele al sottosistema `parport`, in modo da fare funzionare *contemporaneamente* diversi dispositivi collegati in seria (e.g. un lettore ZIP da porta parallela ed una stampante) connessi ad *una* porta parallela. Il conteggio dei file di dispositivo per stampanti alla porta parallela inizia con `/dev/lp0`. Per poter stampare tramite la prima porta parallela, con il kernel standard di SUSE si devono caricare i moduli `parport`, `parport_pc` e `lp`. Questo viene fatto di solito automaticamente da kmod *Kernel Module Loader*, non appena si accede per la prima volta ad un file di dispositivo (e.g. `/dev/lp0`).

Se il modulo del kernel `parport_pc` viene caricato senza parametri speciali, esso cercherà di rilevare e configurare automaticamente la porta parallela. In casi rari ciò non funziona, e si può verificare un improvviso blocco del sistema. A questo punto bisogna configurare i parametri corretti per il modulo `parport_pc` esplicitamente a mano. Per tale motivo, come descritto nella sezione 5.3 a pagina 103, con YaST2 si lascia evitare il rilevamento automatico della stampante.

Configurazione manuale dell'interfaccia parallela

La porta parallela `/dev/lp0` viene configurata attraverso una registrazione in `/etc/modules.conf` (file 6.1).

Exempio 6.1: */etc/modules.conf: prima porta parallela*

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=none
```

Accanto ad `io` si vede l'indirizzo IO della porta parallela. Accanto ad `irq` c'è `none` quale preimpostazione per il funzionamento nella modalità polling o l'interrupt delle porte parallele. Il polling è meno problematico dell'interrupt, dal momento che si possono evitare dei conflitti di interrupt. Comunque vi sono delle schede madri e/o stampanti che funzionano correttamente solo nella modalità Interrupt; inoltre questa modalità fa sì che la stampante riceva abbastanza dati anche se il sistema lavora sotto carico.

Affinché queste impostazioni funzionino, nel BIOS o attraverso il firmware del PC dovrete impostare per la porta parallela i seguenti valori (se disponibili):

- Indirizzo IO `378` (esadecimale)
- Interrupt `7` (irrelevante nella modalità polling)
- Modo `Normal`, `SPP` o `Output-Only` (altre modalità non sempre funzionano)
- `DMA` è disabilitato (lo dovrebbe essere nella modalità `Normal`)

Se l'Interrupt `7` è ancora libero, allora la modalità interrupt può essere attivata nel file 6.2.

Exempio 6.2: */etc/modules.conf: modalità Interrupt per la prima porta parallela*

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

Prima di attivare la modalità interrupt, bisogna vedere nel file `/proc/interrupts` quali interrupt vengono già utilizzati, laddove qui vengono indicati solo gli interrupt attualmente in uso, cosa che può variare in base all'uso attivo di componenti hardware. L'interrupt per la porta parallela non può essere già utilizzato. In caso di dubbio, utilizzate la modalità polling.

Abilitazione e test di una porta parallela

Dopo il riavvio, sarà pronta l'interfaccia parallela. Invece di un reboot, basta attualizzare, come utente `root`, la lista delle dipendenze dei moduli del kernel e scaricare i moduli del kernel necessari all'interfaccia parallela…

```
depmod -a 2>/dev/null
rmmod lp
rmmod parport_pc
rmmod parport
```

... e ricaricare:

```
modprobe parport
modprobe parport_pc
modprobe lp
```

Se la stampante emette testo ASCII, come utente `root` tramite il seguente comando dovreste essere in grado di stampare con il seguente comando una pagina con la parola `Hello`:

```
echo -en "\rHello\r\f" >/dev/lp0
```

La parola `Hello` è, nell'esempio, affiancata dal simbolo ASCII `\r` che codifica il capoverso e seguita dal simbolo ASCII `\f` che codifica un avanzamento di modulo spesso abbreviato con FF (per formfeed).

6.1.2 Interfaccia USB

Nel BIOS del computer, deve essere attivato un interrupt per l'USB. Con un Award-BIOS, per esempio, si deve impostare 'USB IRQ' nel menu 'PNP AND PCI SETUP' su `Enabled`. A seconda della versione BIOS vengono utilizzati anche altri termini.

Eseguite un test per vedere se la stampante USB è indirizzabile, immettendo come utente `root`:

```
echo -en "\rHello\r\f" >/dev/usb/lp0
```

Se una sola stampante USB è collegata e la stampante è in grado di stampare caratteri ASCII, dovrebbe venire stampata una pagina con la parola `Hello`.

Alcune stampanti USB necessitano una sequenza di controllo speciale, prima di accettare dati tramite USB. Per maggiori informazioni consultate anche la banca dati di supporto `http://sdb.suse.de/en/sdb/html` immettendo la parola chiave Epson ed usb.

Nell'output del seguente comando dovrebbe esservi il produttore e il nome della stampante:

```
cat /proc/bus/usb/devices
```

Se non vengono indicati né il produttore né il prodotto, di solito sono queste le cause:

- Il sistema USB non ha (ancora) rilevato il dispositivo – forse perché la stampante USB è spenta. La stampante USB allora non è indirizzabile.
- Il sistema USB ha sì rilevato il dispositivo, ma non conosce né il produttore né il nome della stampante e quindi non mostra nulla. La stampante USB è comunque indirizzabile.

A volte succede che la stampante USB risulta non indirizzabile (per esempio, se si stacca lo spinotto USB durante un processo di stampa). Di solito, dovrebbero bastare questi comandi per riavviare il sistema USB:

```
rchotplug stop
rchotplug start
```

Se non ciò non dovesse bastare, terminate tutti i processi che accedono a `/dev/usb/lp0` e scaricate e ricaricate i moduli del kernel che riguardano le stampanti USB. Con `lsmod` controllate prima quali moduli USB siano caricati (se `usb-uhci` o `usb-ohci` o `uhci`) o se ci siano ancora altre dipendenze di moduli, ad esempio la seguente segnalazione indica che il modulo `usbcore` è ancora richiesto dai moduli `printer` e `usb-uhci`:

```
usbcore ... [printer usb-uhci]
```

In questo caso, prima del modulo `usbcore`, devono venire scaricati i moduli `printer` ed `usb-uhci`. Immettete come utente `root` i seguenti comandi (al posto di `usb-uhci` a secondo del sistema anche `uhci` o `usb-ohci`):

```
fuser -k /dev/usb/lp0
rchotplug stop
rmmod printer
rmmod usb-uhci
umount usbdevfs
rmmod usbcore
modprobe usbcore
mount usbdevfs
modprobe usb-uhci
modprobe printer
rchotplug start
```

Se sono connesse diverse stampanti USB, bisogna considerare quanto segue: il sottosistema USB rivela automaticamente stampanti USB connesse. La prima stampante USB rilevata, è indirizzabile tramite il dispositivo `/dev/usb/lp0`. La seconda stampante USB rilevata, è indirizzabile tramite il dispositivo `/dev/usb/lp1`. Alcuni modelli di stampante vengono rilevati automaticamente anche quando sono spente; ciò è dovuto al fatto che alcune stampanti anche spente, possono essere interrogate tramite il collegamento USB. Per evitare di perdere la vista di insieme per quanto riguarda i dispositivi USB, prima di avviare Linux tutte le stampanti USB dovrebbero essere accese e possibilmente rimanere tali durante tutta la fase di funzionamento.

6.1.3 Interfaccia della stampante IrDA

Una interfaccia parallela viene emulata tramite il collegamento ad infrarossi. Il driver nel kernel Linux mette a disposizione un'interfaccia parallela simulata sotto il dispositivo `/dev/irlpt0`. Una stampante dunque viene indirizzata tramite l'interfaccia ad infrarossi allo stesso modo di una stampante connessa alla porta parallela con la sola differenza che viene utilizzato `/dev/irlpt0` al posto di `/dev/lp0`.

Eseguite un test se la stampante IrDA risulta indirizzabile immettendo come `root`:

```
echo -en "\rHello\r\f" >/dev/irlpt0
```

Premesso che la stampa riesca a stampare caratteri ASCII, allora dovrebbe venir prodotta una pagina con la parola `Hello`.

Ad ogni caso la stampante dovrebbe apparire nell'output del seguente comando: `irdadump`. Se il comando irdadump non esiste, allora bisogna installate il `irda`, altrimenti la stampante non è indirizzabile. Se non viene indicato proprio niente, allora probabilmente il servizio di sistema IrDA non sarà stato inizializzato, perché non viene inizializzato automaticamente all'avvio. Il servizio di sistema IrDA si inializza e termina con i seguenti comandi:

```
rcirda start
rcirda stop
```

6.1.4 Interfacce seriali

Il funzionamento della stampante collegata ad un'interfaccia seriale per quanto riguarda lo spooler viene descritto nel *LPRng-Howto* sotto `file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html` e lì in particolar modo in `file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#SECSERIAL` e nella la pagina di manuale printcap. Nella banca dati di supporto trovate ulteriori informazioni avviando una ricerca immettendo il termine serial.

6.2 Configurazione manuale di LPRng/lpdfilter

Di solito il sistema di stampa viene configurato con YaST2, come descritto nella sezione 5.3 a pagina 103. Inoltre per il sistema di stampa LPRng/lpdfilter LPRng/lpdfilter vi è il programma lprsetup basato sulla riga di comando.

Quando una stampante viene configurata con YaST2, esso raccoglie le informazioni necessarie e richiama lprsetup per la configurazione del sistema di stampa LPRng/lpdfilter con le opzioni necessarie da applicare.

Il programma lprsetup è stato ideato come tool per esperti. A differenza di YaST2, lprsetup non aiuta l'utente a trovare i valori giusti per le singole opzioni. Con `lprsetup -help` vengono elencate e descritte le opzioni possibili, e ulteriori informazioni sono reperibili nelle le pagine di manuale lprsetup o lpdfilter.

Per reperire delle informazioni su driver Ghostscript e parametri specifici del driver vedi sezione 5.2.2 a pagina 100 e 6.6 a pagina 165.

6.3 Lo spooler della stampante LPRng

Come spooler della stampante del sistema di stampa LPRng/lpdfilter viene utilizzato LPRng (`lprng`).

Lo spooler della stampante lpd *Line Printer Daemon* normalmente viene attivato automaticamente all'avvio del sistema, richiamando lo script `/etc/init.d/lpd`. Manualmente lo spooler della stampante - che gira come demone in background ovvero in sottofondo - può essere inizializzato e terminato con:

```
rclpd start
rclpd stop
```

Il file di configurazione per LPRng:

/etc/printcap Configurazione delle singole code di stampa

/etc/lpd.conf Configurazione globale dello spooler

/etc/lpd.perms Configurazione dei permessi di accesso

Con `rclpd start` viene invocato in base a `/etc/init.d/lpd` anche `checkpc -f` che genera le directory spool `/var/spool/lpd/*` attenendosi alle registrazioni in `/etc/printcap` ed imposta di conseguenza i permessi d'accesso.

Lo spooler della stampante stabilisce all'avvio, basandosi sulle registrazioni in `/etc/printcap` quali code di stampa sono definite. Il suo compito è quello di organizzare l'esecuzione di incarichi temporaneamente memorizzati:

- Amministra le code di stampa locali e invia i file dati di un incarico attraverso il filtro della stampante e in seguito o direttamente alla stampante o li inoltra ad una coda di stampa diversa.
- Tiene in considerazione la successione degli incarichi nelle code di stampa.
- Controlla lo stato delle code di stampa e della stampante, e fornisce le informazioni richiesti.
- Ascolta alla porta `515`, se sono in arrivo incarichi per la stampante da computer remoti per le code di stampa locali da accettare o eventualmente da rifiutare.
- Inoltra gli incarichi da stampare allo spooler di computer remoti (dunque la porta `515`) al computer remoto.

Per i dettagli sullo spooler LPRng leggete *LPRng-Howto* sotto `file: /usr/share/doc/packages/lprng/LPRng-HOWTO.html` le pagine di manuale printcap e lpd.

6.3.1 Stampare da applicativi

Gli applicativi utilizzano in questo caso il comando `lpr` per stampare. Inoltre scegliete nell'applicativo un nome di una coda di stampa esistente (e.g. `color`) oppure immettete nella maschera di stampa dell'applicativo il comando per stampare adatto (e.g. `lpr -Pcolor`)..

Con la riga di comando si stampa attraverso il comando `lpr -Plp` ⟨*`NOMEFILE`*⟩, dove ⟨*NOMEFILE*⟩ va sostituito con il nome del file da stampare. Attraverso l'opzione `-P` si può determinare esplicitamente la coda di stampa. Con `lpr -Pcolor NOMEFILE` viene usata per esempio la coda di stampa `color`.

6.4 Tool della riga di comando per LPRng

I tool di riga di comando vengono descritti dettagliatamente nel *LPRng-Howto* sotto `file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#LPRNGCLIENTS`,così qui riportiamo solo un breve riassunto:

6.4.1 Per code di stampa locali

Generare incarichi di stampa

Il comando `lpr` viene descritto nel *LPRng-Howto* sotto `file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#LPR`, in questa sede riportiamo solo le nozioni fondamentali:

Di solito si stampa con `lpr -P` ⟨*`coda di stampa`*⟩ ⟨*`file`*⟩. Omettendo l'opzione `-P`⟨*`coda di stampa`*⟩ , il default è il contenuto della variabile di ambiente `PRINTER`. Questo vale anche per i comandi `lpq` e `lprm` – vedi le pagine di manuale relative a lpr, lpq e lprm. La variabile di ambiente `PRINTER` viene impostata automaticamente al login, e può essere visualizzata con il comando `echo $PRINTER` e con `export PRINTER=`⟨*`coda di stampa`*⟩ venir impostata su un'altra coda di stampa.

Visualizzare lo stato

`lpq -P`⟨*`coda di stampæ`*⟩ mostra gli incarichi per la stampa nella coda di stampa indicata. Come nel caso dello spooler LPRng immettete `all` come coda, e vengono elencati tutti gli incarichi di tutte le code di stampa.

Con `lpq -s -P`⟨*coda di stampa*⟩ vengono mostrate poche informazioni; con `lpq -l -P`⟨ *coda di stampa*⟩ le informazioni fornite sono più corpose.

Con `lpq -L -P`⟨*coda di stampa*⟩ viene emesso un rapporto dettagliato sullo stato che serve alla individualizzazione di fonti di errore.

Per ulteriori informazioni vedi sotto la sezione *Mostra lo stato di queue remote*, la ed infine `file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#LPQ` nel *LPRng-Howto*.

Cancellare incarichi di stampa

Con `lprm -P`⟨*coda di stampa*⟩ ⟨*numero dell'incarico*⟩ si cancella l'incarico specificato dalla coda di stampa indicata se l'incarico appartiene all'utente che ha immesso il comando `lprm`. L'incarico appartiene all'utente sul computer che ha inviato l'incarico. Questo utente si lascia identificare con il comando `lpq` che mostra anche il numero dell'incarico.

Con il comando `lprm -Pall all` vengono cancellati tutti gli incarichi di tutte le code di stampa per i quali ne ha il permesso l'utente che ha immesso il comando `lprm`. L'utente `root` può cancellare ogni incarico (di tutte le queue).

Per ulteriori informazioni consultate la pagina di manuale lprm e sotto `file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#LPRM` nell'*LPRng-Howto*.

Controllo delle code di stampa

Il comando `lpc option` ⟨*coda di stampa*⟩ mostra lo stato delle code di stampa indicate e permette di modificarle. Le opzioni principali sono:

`help` dà un sommario delle opzioni.

`status` ⟨***coda di stampa***⟩ dà una panoramica sullo stato.

`disable` ⟨***coda di stampa***⟩ ferma l'assunzione di nuovi incarichi nella coda di stampa.

`enable` ⟨***coda di stampa***⟩ abilita la coda di stampa ad accettare nuovi incarichi.

`stop` ⟨***coda di stampa***⟩ ferma il processo di stampa degli incarichi della coda di stampa; l'incarico che si trova in fase di stampa viene ancora terminato.

start ⟨***coda di stampa***⟩ riprende con il stampare degli incarichi della coda di stampa.

down ⟨***coda di stampa***⟩ ha l'effetto di `disable` più `stop`

up ⟨***coda di stampa***⟩ ha l'effetto di `enable` più `start`.

abort ⟨***coda di stampa***⟩ è identico a `down`, con la sola differenza che l'incarico che si trova in fase di stampa viene interrotto immediatamente. Questi incarichi rimangono validi e possono essere terminati dopo un riavvio della coda di stampa (`up`).

Per apportare delle modifiche alle code di stampa vi servono i permessi di `root`.Potete immettere i comandi nella riga di comando (e.g. `lpc status all`), o invocare `lpc` senza parametri: viene inizializzato il modo dialogo con il prompt `lpc>` che aspetta l'immissione delle opzioni riportate sopra. Con `quit` o `exit` terminate il dialogo.

Se `lpc status all` ad esempio emette

```
Printer        Printing Spooling Jobs Server Subserver
lp@earth        enabled  enabled    2    123       456
color@earth    disabled disabled    0   none      none
laser@earth    disabled  enabled    8   none      none
```

vuol dire che la queue `lp` è attivata e contiene due incarichi, di cui uno si trova in fase di stampa. La coda di stampa `color` è disattivata. Nella coda di stampa `laser`, e.g. per motivi di manutenzione della stampante, è disattivata solo l'emissione delle pagine stampate, ma è possibile continuare a generare degli incarichi che finiranno sulla coda di stampa (nel nostro esempio: 8).

Per ulteriori informazioni consultate la pagina di manuale lpc e sotto `file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#LPC` nell'*LPRng-Howto*.

6.4.2 Per queue remote

Qui dovete sostituire `<server di stampa>` con il nome o l'indirizzo IP del server di stampa, e `<coda di stampa>` deve essere una coda di stampa sul server di stampa.

Generare incarichi di stampa

Con lo spooler LPRng si può accedere a code remote con il comando `lpr` anche su code di stampa remote nel seguente modo: `lpr -P`⟨*`coda di stampa`*⟩`@`⟨*`server di stampa`*⟩ ⟨*`file`*⟩. La premessa è che il server di stampa sia stato configurato in modo che sia possibile utilizzare le sue code di stampa, cosa possibile di default con LPRng.

Visualizzare lo stato

Con i seguenti comandi potete interrogare code di stampa remote:

```
lpq -P<coda di stampa>@<server di stampa>
lpq -s -P<coda di stampa>@<server di stampa>
lpq -l -P<coda di stampa>@<server di stampa>
lpq -L -P<coda di stampa>@<server di stampa>
```

e

```
lpc status <coda di stampa>@<server di stampa>
lpc status all@<server di stampa>
```

Soprattutto con `lpq -s -Pall@`⟨*`server di stampa`*⟩ o `lpc status all@`⟨*`server di stampa`*⟩ possono venire rilevati i nomi di tutte le code di stampa sul server di stampa, se anche sul server di stampa viene utilizzato LPRng.

Se non è possibile stampare su code remote, una interrogazione sullo stato può dare utili indicazioni. Con `lpq -L -P`⟨*`coda di stampa`*⟩`@`⟨*`server di stampa`*⟩ può essere visualizzato un rapporto sullo stato ai fini della diagnosi da remoto, se sul server di stampa viene utilizzato LPRng.

Cancellare incarichi di stampa

Con i seguenti comandi potrete cancellare tutti gli incarichi su queue remote che avete generato:

```
lprm -P<coda di stampa>@<server di stampa> <numero dell'incarico>
lprm -P<coda di stampa>@<server di stampa> all
lprm -Pall@<server di stampa> all
```

Considerate che `root` non dispone di permessi speciali per quel che riguarda code remote. `all` funziona solo se anche sul server di stampa venga utilizzato LPRng.

6.4.3 Eliminare delle disfunzioni in LPRng con i comandi di sopra

Gli incarichi di stampa rimangono validi nella coda di stampa se durante un processo di stampa spegnete il computer ed riavviate Linux – eventualmente un incarico di stampa contenente degli errori va rimosso dalla coda di stampa ricorrendo ad uno dei comandi sopra descritti.

Se e.g. si verifica un guasto per quanto riguarda la comunicazione tra computer e stampante, la stampante non è in grado di elaborare i dati che le sono stati inviati e come risultato vengono riempiti innumerevoli fogli con caratteri privi di significato.

1. Con stampanti a getto di inchiostro togliete innanzitutto i fogli o nel caso di stampanti laser aprite il cassetto dei fogli per fermare il processo di stampa.
2. Visto che l'incarico viene rimosso dalla coda di stampa solo dopo essere stato inviato completamente alla stampante, lo si ritroverà nella maggior parte dei casi ancora nella coda di stampa. Controllate con `lpq` o `lpc status` quale incarico di quale coda si trova attualmente nel processo di stampa, e cancellate l'incarico con `lprm`.
3. Può verificarsi che vengono trasmessi dei dati alla stampante anche se l'incarico è stato cancellato dalla coda di stampa. Tutti processi che accedono ancora alla stampante vengono terminati con il comando `fuser -k /dev/lp0` per stampanti alla porta parallela e con `fuser -k /dev/usb/lp0` per una stampante USB.
4. Eseguite un reset della stampante staccando per alcuni minuti la spina, ed in seguito rimettete i fogli e accendete la stampante.

6.5 Il filtro della stampante del sistema di stampa LPRng/lpdfilter

Come filtro della stampante viene utilizzato lpdfilter (il pacchetto `lpdfilter`). Segue una descrizione dettagliata della elaborazione di un incarico di stampa. Per una analisi dettagliata dei filtri, leggete i script del filtro (in particolare `/usr/lib/lpdfilter/bin/if`) ed eventualmente procedete come descritto nella sezione 6.5.3 a pagina 164.

1. Il filtro (`/usr/lib/lpdfilter/bin/if`) determina le opzioni che gli sono stati passati dallo spooler, o le legge dal cosiddetto control file dell' incarico, nonché, a seconda delle coda di stampa, dai file `/etc/printcap` e `/etc/lpdfilter/`⟨*coda di stampa*⟩`/conf` (⟨*coda di stampa*⟩ va sostituito con il nome effettivo della coda).

2. Se si tratta di una coda di stampa `ascii`, il filtro viene forzato a trattare i dati da stampare come caratteri ASCII. Se non si tratta di una coda di stampa `ascii`, il filtro cerca di determinare automaticamente il tipo di dati da stampare. Il tipo di dati da stampare viene determinato dallo script `/usr/lib/lpdfilter/bin/guess` che applica il comando `file` ai dati da stampare, e a mano del suo output viene determinato il tipo di dati da stampare in base alle indicazioni nel file `/etc/lpdfilter/types`.

3. A seconda del tipo di dati e di coda, avviene la conversione in dati specifici da stampare:

   - Se si tratta di una coda `raw`, i dati da stampare vengono inviati direttamente alla stampante (o ad un'altra coda); se le impostazioni in `/etc/lpdfilter/`⟨*coda di stampa*⟩`/conf` lo prevedono, essi possono anche venire ricodificati con recode. Per una coda di stampa puramente `raw` (ovvero senza lpdfilter), cancellate per la coda in questione, la riga `:if=/usr/lib/lpdfilter/bin/if:\`.
   - Se non si tratta di una coda di stampa `raw`:
     (a) Se i dati da stampare non sono di natura PostScript, lo diventeranno richiamando `/usr/lib/lpdfilter/filter/tipo2ps` (laddove `tipo` va sostituito dal tipo di dati da stampare). I testi ASCII, in particolare, vengono convertiti in PostScript con il programma a2ps in base a `/usr/lib/lpdfilter/filter/ascii2ps` e secondo la codificazione della lingua configurata per la coda di stampa. In questo modo, tutti i caratteri speciali propri di una lingua potranno essere stampati correttamente anche in semplice formato di testo; vd. anche la pagina di manuale a2ps.
     (b) Eventualmente è anche possibile riformattare i dati PostScript, a condizione che, sotto `/etc/lpdfilter/`⟨*coda di stampa*⟩`/pre` vi sia uno script adatto (laddove ⟨*coda di stampa*⟩ è da sostituire con il nome della coda).
     (c) I dati PostScript possono essere convertiti anche in un altro linguaggio della stampante.

- ▷ Se avete una stampante PostScript, i dati in PostScript vengono inviati direttamente ad essa (o ad un'altra coda). Tuttavia, potrebbero venire attivate inoltre le funzioni bash duplex e tray, definite in `/usr/lib/lpdfilter/global/functions`, per permettere la stampa duplex o la scelta di un determinato cassetto dei fogli tramite comandi PostScript (a condizione che la stampante PostScript processi questi comandi).
- ▷ Se non avete collegato una stampante PostScript, Ghostscript verrà usato con un driver adatto al linguaggio del modello della stampante, per poter generare i dati da potere essere inviati alla stampante (o ad un'altra coda di stampa).
  Troverete i parametri per aprire Ghostscript in `/etc/printcap` direttamente nella riga `cm` o nel file `/etc/lpdfilter/` ⟨*coda di stampa*⟩`/upp` (sostituite `coda di stampa` con il nome effettivo della coda di stampa).
  L'output di Ghostscript può essere anche riformattato, a condizione che `/etc/lpdfilter/`⟨*coda di stampa*⟩`/post` contenga uno script adatto (sostituite ⟨*coda di stampa*⟩ con il nome della coda di stampa).

(d) I dati da stampare vengono spediti alla stampante (o ad un'altra coda di stampa). Assieme ad essi, potete anche inviare, prima o dopo i dati da stampare, delle sequenze di controllo specifiche, se le avete registrate in `/etc/lpdfilter/` ⟨*coda di stampa*⟩`/conf`.

6.5.1 Configurazione di lpdfilter

Normalmente il sistema di stampa viene configurato con YaST2 come descritto nella sezione 5.3 a pagina 103, e soprattutto viene configurato in tal modo anche l'lpdfilter.

Per impostazioni speciali dovete adattare manualmente i file di configurazione del filtro della stampante.Ogni coda di stampa ha il proprio file di configurazione `/etc/lpdfilter/`⟨*coda di stampa*⟩ `/conf` (sostituite ⟨*coda di stampa*⟩ con il nome effettivo della coda) che contiene inoltre delle informazioni su ogni opzione.

6.5.2 Aggiunte personali all' lpdfilter

1. Se i dati da stampare non sono in PostScript, vengono convertiti in PostScript invocando `/usr/lib/lpdfilter/filter/tipo2ps` laddove `tipo` va sostituto con il tipo di dati da stampare).

   Se sotto `/etc/lpdfilter/`⟨*coda di stampa*⟩`/tipo2ps` si trova uno script adatto, verrà utilizzato per convertire i dati da stampare in PostScript. Questo script riceve i dati da stampare tramite `stdin` e li emette tramite `stdout` in formato PostScript.

2. I dati PostScript possono anche essere riformattati ancora, a condizione che in `/etc/lpdfilter/`⟨*coda di stampa*⟩`/pre` vi sia uno script adatto. Potete aggiungere anche i vostri PostScript preload tramite uno script adatto. Questo script riceve i dati di stampa tramite `stdin` e li emette tramite `stdout` in formato PostScript. Applicazioni per riformattare dati PostScript, si trovano nel pacchetto `psutils`. In particolar modo pstops consente un'ampia riformattazione; vedi a riguardo la pagina di manuale pstops.

3. Parametri speciali per Ghostscript: durante la configurazione con YaST2, vengono memorizzati i parametri per la chiamata di Ghostscript nel file `/etc/lpdfilter/` ⟨*coda di stampa*⟩`/upp` (sostituite ⟨*coda di stampa*⟩ con il nome effettivo della coda). In questo file potete inserire manualmente anche dei parametri speciali per Ghostscript. Vd. anche la sezione 6.6 a pagina 165.

4. Anche l'output di Ghostscript può essere riformattato, a condizione che sotto `/etc/lpdfilter/`⟨*coda di stampa*⟩ `/post` vi sia uno script adatto (sostituite ⟨*coda di stampa*⟩ con il nome effettivo della coda di stampa). Questo script riceve l'output di Ghostscript tramite `stdin` e emette i dati da stampare tramite `stdout`.

Un esempio che prescinde dall'hardware

Presupponendo che vi sia una coda di stampa `test`, tramite la quale debba essere stampato un testo ASCII con righe numerate e nella quale ogni foglio debba contenere due pagine ridotte. In questo caso, si possono creare i seguenti script: `/etc/lpdfilter/test/ascii2ps` ed `/etc/lpdfilter/test/pre`.

Exempio 6.3: */etc/lpdfilter/test/ascii2ps: conversione di ASCII in PostScript*

```
#!/bin/bash
cat -n - | a2ps -1 --stdin=' ' -o -
```

Exempio 6.4: */etc/lpdfilter/test/pre: riformattare PostScript*

```
#!/bin/bash
pstops -q '2:0L@0.6(20cm,2cm)+1L@0.6(20cm,15cm)'
```

Questi script devono essere eseguibili per ogni utente, cosa che si realizza tramite comando `chmod`:

```
chmod -v a+rx /etc/lpdfilter/test/ascii2ps
chmod -v a+rx /etc/lpdfilter/test/pre
```

`pstops` funziona solo per file PostScript creati in modo da consentire la riformattazione (cosa normalmente consentita).

Utilizzare propri PostScript preload

I cosiddetti PostScript-preload sono dei piccoli file che contengono comandi PostScript speciali che vengono anteposti ai dati da stampare veri e propri, per poter inizializzare in modo adeguato una stampante PostScript o Ghostscript con questi comandi speciali. Normalmente, i PostScript preload vengono utilizzati per attivare la stampa duplex con stampanti PostScript o per selezionare determinati cassetti dei fogli oppure per impostare i margini e le correzioni gamma.

L'importante è che la stampante PostScript o Ghostscript possa elaborare i comandi PostScript sotto descritti (Ghostscript non reagisce a comandi per stampa duplex o cassetto dei fogli).

Supponiamo che la relativa coda di stampa sia `test`.

Stampa duplex Per attivare e disattivare la stampa duplex, potete creare i seguenti file: `/etc/lpdfilter/test/duplexon.ps` e `/etc/lpdfilter/test/duplexoff.ps`:

Exempio 6.5: */etc/lpdfilter/test/duplexon.ps: attivare stampa duplex*

```
%!PS
statusdict /setduplexmode known
{statusdict begin true setduplexmode end} if {} pop
```

Exempio 6.6: */etc/lpdfilter/test/duplexoff.ps: disattivare la stampa duplex*

```
%!PS
statusdict /setduplexmode known
{statusdict begin false setduplexmode end} if {} pop
```

Per ruotare il retro di una pagina stampata in duplex, utilizzate il seguente codice PostScript:

```
%!PS
statusdict /setduplexmode known
{statusdict begin true setduplexmode end} if {} pop
statusdict /settumble known
{statusdict begin true settumble end} if {} pop
```

Selezione del cassetto della carta Per attivare il cassetto della carta standard con la cifra 0 o il cassetto e.g. con la cifra 2, potete creare i seguenti file `/etc/lpdfilter/test/tray0.ps` e `/etc/lpdfilter/test/tray2.ps`:

Exempio 6.7: */etc/lpdfilter/test/tray0.ps: abilitare il cassetto 0*

```
%!PS
statusdict /setpapertray known
{statusdict begin 0 setpapertray end} if {} pop
```

Exempio 6.8: */etc/lpdfilter/test/tray2.ps: abilitare il cassetto 2*

```
%!PS
statusdict /setpapertray known
{statusdict begin 2 setpapertray end} if {} pop
```

Impostazioni dei margini Per modificare i margini, potete creare il seguente file `/etc/lpdfilter/test/margin.ps`:

Exempio 6.9: */etc/lpdfilter/test/margin.ps: impostazioni dei margini*

```
%!PS
<<
/.HWMargins [left bottom right top]
/PageSize [width height]
/Margins [left-offset top-offset]
>>
setpagedevice
```

Le impostazioni dei margini `left`, `bottom`, `right` e `top` e le dimensioni del foglio `width` e `height` sono espressi in "punti" (laddove un punto corrisponde a 1/72 pollici o circa 0.35 mm). Gli offset `left-offset` e `top-offset` vengono espressi in punti di matrice e dipendono quindi dalla risoluzione. Per spostare la posizione della stampa sul foglio, basta il file `/etc/lpdfilter/test/offset.ps`

Exempio 6.10: */etc/lpdfilter/test/offset.ps: posizionamento del testo stampato*

```
%!PS
<< /Margins [left-offset top-offset] >> setpagedevice
```

Correzione gamma Per modificare la distribuzione della luminosità dei colori, create i file `/etc/lpdfilter/test/cmyk.ps` ed `/etc/lpdfilter/test/rgb.ps`:

Exempio 6.11: */etc/lpdfilter/test/cmyk.ps: correzione gamma CMYK*

```
%!PS
{cyan exp} {magenta exp} {yellow exp} {black exp}
setcolortransfer
```

Exempio 6.12: */etc/lpdfilter/test/rgb.ps: correzione gamma RGB*

```
%!PS
{red exp} {green exp} {blue exp} currenttransfer
setcolortransfer
```

Il modello di colore (CMYK o RGB) deve adattarsi alla vostra stampante. I valori da impostare per `cyan`, `magenta`, `yellow`, `black`, `red`, `green` e `blue`, possono essere determinati a seguito di test. Comunque dovranno essere tra `0.001` e `0.999`. Potete verificare l'effetto dei file sopradescritti con l'interfaccia grafica, allo schermo, senza correzioni gamma:

```
gs -r60 \
/usr/share/doc/packages/ghostscript/examples/colorcir.ps
```

Con correzione gamma uno di questi esempi:

```
gs -r60 /etc/lpdfilter/test/cmyk.ps \
    /usr/share/doc/packages/ghostscript/examples/colorcir.ps
gs -r60 /etc/lpdfilter/test/rgb.ps \
    /usr/share/doc/packages/ghostscript/examples/colorcir.ps
```

Uscite con Ctrl + c.

Resettare la stampante Per riportare la stampante alle impostazioni di default, potete creare il seguente file `/etc/lpdfilter/test/reset.ps`:

Exempio 6.13: *`/etc/lpdfilter/test/reset.ps`: risettare la stampante*

```
%!PS
serverdict begin 0 exitserver
```

Per attivare un file PostScript-preload, potete creare il seguente script `/etc/lpdfilter/test/pre`:

Exempio 6.14: *`/etc/lpdfilter/test/pre`: caricare PostScript-preload*

```
#!/bin/bash
cat /etc/lpdfilter/test/preload.ps -
```

Sostituite `preload.ps` con il nome del file preload adatto. Lo script deve essere eseguibile e il file preload leggibile per tutti gli utenti, ciò viene realizzato con il comando `chmod`:

```
chmod -v a+rx /etc/lpdfilter/test/pre
chmod -v a+r /etc/lpdfilter/test/preload.ps
```

Potete usare lo stesso meccanismo per inviare un file PostScript alla stampante non solo prima, ma anche dopo i veri e propri dati di stampa PostScript. Ad esempio, per resettare la stampante alla fine di un incarico di stampa, potete apportare le seguente aggiunte allo script `/etc/lpdfilter/test/pre`:

Exempio 6.15: *`etc/lpdfilter/test/pre`: PostScript-preload e PostScript-reset*

```
#!/bin/bash
cat /etc/lpdfilter/test/preload.ps - /etc/lpdfilter/test/reset.ps
```

Esempio di configurazione di una stampante cosiddetta GDI

Volete impostare una coda di stampa `gdi` per una stampante GDI. Questo tipo di stampanti normalmente non può essere usato con Linux, vd. la sezione 5.2.3 a pagina 101.Tuttavia esistono per alcune stampanti GDI speciali programmi driver che normalmente vengono utilizzati come complemento per Ghostscript, convertendo l'output di Ghostscript nel formato adatto alla stampante. Questo tipo di programmi driver comportano spesso delle restrizioni per quanto riguarda la stampa – e.g. stampano solo in bianco e nero. Ghostscript e i programmi driver si completano a vicenda come segue (cfr. il paragrafo 6.6 a pagina 165.)

1. I dati PostScript vengono risolti da Ghostscript in una matrice di tanti punti. I dati della matrice vengono poi riprodotti, tramite un programma driver collegato in serie adatto al driver Ghostscript, ed emessi nel formato giusto e con la risoluzione giusta.
2. I dati della matrice vengono convertiti nel formato della stampante attraverso il programma driver.

Si parte qui dal presupposto che disponete di un programma driver per la stampante adatto alla vostra versione di SUSE LINUX o esso che possa essere scaricato dall'Internet. Si presuppone inoltre che il programma driver funzioni come descritto sopra, e che voi sappiate usare in Unix e.g. archivi `.zip` o `.tar.gz` oppure pacchetti `.rpm`.

Dopo aver decompresso un tale archivio, troverete delle istruzioni all'installazione in file di nome `README` o in una sottodirectory di nome `doc`. Nel caso degli archivi `.tar.gz`, il programma driver vero e proprio deve essere compilato ed installato.

Nel seguente esempio si parte dal presupposto:

- Il programma driver è `/usr/local/bin/printerdriver`.
- Quale driver Ghostscript è richiesto `pbmraw` con una risoluzione di `600` dpi.
- La stampante è collegata alla prima porta parallela `/dev/lp0`.

Quale driver Ghostscript e quale risoluzione utilizzare effettivamente viene indicato nella documentazione del programma driver.

Per prima cosa, create la queue `gdi` con lprsetup (come `root`):

```
lprsetup -add gdi -lprng -device /dev/lp0 \
    -driver pbmraw -dpi 600 -size a4dj -auto -sf
```

Quindi va generato il seguente script `/etc/lpdfilter/gdi/post`:

```
#!/bin/bash
/usr/local/bin/printerdriver <parametri_driver>
```

Eventualmente inserire i ⟨*parametri_specifici_del_driver*⟩ adatti. Quali parametri specifici del driver utilizzare effettivamente viene indicato nella documentazione del programma driver. Lo script deve poter essere eseguito da tutti gli utenti; infine, riavviare lo spooler:

```
chmod -v a+rx /etc/lpdfilter/gdi/post
rclpd stop
rclpd start
```

Ora ogni utente può stampare con:

```
lpr -Pgdi <file>
```

6.5.3 Debug con lpdfilter

Per attivare il livello di debug giusto, eliminate il simbolo di commento davanti alla riga corrispondente nello script principale `/usr/lib/lpdfilter/bin/if` del filtro della stampante.

Exempio 6.16: */usr/lib/lpdfilter/bin/if: livello di debug*

```
# DEBUG="off"
# DEBUG="low"
# DEBUG="medium"
# DEBUG="high"
```

Con `DEBUG="low"`, verrà salvato solo l'output `stderr` di `/usr/lib/lpdfilter/bin/if` in un file `/tmp/lpdfilter.if-$$.XXXXXX` (sostituite `$$` con il numero del processo; e `XXXXXX` con una combinazione di cifre casuale ma univoca).

Con `DEBUG="medium"`, vengono salvati anche gli output `stderr` degli script sotto `/usr/lib/lpdfilter/filter/` che vengono caricati con `/usr/lib/lpdfilter/bin/if`. Essi vengono memorizzati in file del tipo `/tmp/lpdfilter.nome-$$.XXXXXX` (laddove `nome` è da sostituire con il nome dello script invocato e `$$.XXXXXX` con una combinazione di cifre casuale ma univoca).

Con `DEBUG="high"`, l'output non viene inviato alla stampante, ma memorizzato in un file del tipo `/tmp/lpdfilter.out-$$.XXXXXX` (dove `$$.XXXXXX` viene sostituito analogamente a quanto descritto sopra).

Per non fare confusione, cancellate questi file prima di ogni test con `rm -v /tmp/lpdfilter*`.

6.6 Ghostscript

Ghostscript accetta dati PostScript e PDF come input e per la conversione in altri formati, esso contiene una serie di driver Ghostscript, chiamati in questo contesto device.

Ghostscript suddivide il processo di conversione in due fasi:

1. I dati PostScript vengono trasformati in una matrice: la grafica scritta in linguaggio PostScript viene cioè scomposta in un reticolo fine di punti d'immagine. Questa fase è uguale per tutti i driver di Ghostscript. Quanto più fine è il reticolo (ovvero, quanto più alta la risoluzione), tanto migliore sarà la qualità della stampa. Tuttavia, un raddoppiamento della risoluzione orizzontale e verticale comporta una quadruplicazione dei punti del reticolo e una quadruplicazione della memoria necessaria.

2. La grafica scomposta in punti di matrice viene ora convertita dal driver scelto nel formato (e.g. linguaggio della stampante) desiderato.

Ghostscript non mette a disposizione solo driver per stampanti. Ghostscript può anche elaborare i file PostScript per l'output sullo schermo o convertirli in file PDF. Per visualizzare comodamente file PostScript allo schermo, usate il programma gv (`gv`), visto che offre una interfaccia utente grafica per Ghostscript.

Ghostscript è un programma molto versatile e ricco di opzioni per la riga di comando. La documentazione principale su Ghostscript oltre alla pagina di manuale gs e alla lista dei driver di Ghostscript è reperibile in:

`file:/usr/share/doc/packages/ghostscript/catalog.devices`

nonché nei file:

`file:/usr/share/doc/packages/ghostscript/doc/index.html` `file:/usr/share/doc/packages/ghostscript/doc/Use.htm` `file:/usr/share/doc/packages/ghostscript/doc/Devices.htm` `file:/usr/share/doc/packages/ghostscript/doc/hpdj/gs-hpdj.txt` `file:/usr/share/doc/packages/ghostscript/doc/hpijs/hpijs_readme.html` `file:/usr/share/doc/packages/ghostscript/doc/stp/README`

Se invocate direttamente Ghostscript dopo l'elaborazione del riga comando si avvia un dialogo con un proprio prompt `GS>`, da chiudere con il comando `quit`.

Il comando di aiuto `gs -h` elenca tutte le opzioni principali e fornisce una lista attuale dei dispositivi supportati, indicando solo la denominazione generale del driver, come `uniprint` o `stp` (se un solo driver supporta una serie di modelli). I file con i parametri per `uniprint` ed i modelli di `stp` sono elencati, uno per uno, in `file:/usr/share/doc/packages/ghostscript/catalog.devices`.

6.6.1 Esempi di impiego di Ghostscript

In `file:/usr/share/doc/packages/ghostscript/examples` trovate file esempi PostScript. L'elisse cromatica `file:/usr/share/doc/packages/ghostscript/examples/colorcir.ps` si adatta bene per un test di stampa.

Output X11

Su X, la superficie grafica, potete visualizzare un file PostScript con il comando `gs`:

```
gs -r60 \
/usr/share/doc/packages/ghostscript/examples/colorcir.ps
```

Con l'opzione `-r`, viene indicata la risoluzione, che dovrà essere adatta al dispositivo in questione (stampante o schermo) (provate con `-r30`). Per chiudere il programma, premete, nella finestra di terminale in cui avete dato il comando `gs`, i tasti Ctrl + c .

Conversione in PCL5e

La conversione di un file PostScript in un formato di stampante PCL5e o PCL6 si realizza con il comando:

```
gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn \
    -sDEVICE=ljet4 -r300x300  \
    /usr/share/doc/packages/ghostscript/examples/colorcir.ps \
    quit.ps
```

laddove il comando dovrà stare in un'unica riga senza (\). Inoltre, si presuppone che il file `/tmp/out.prn` non esista ancora.

Conversione in PCL3

La conversione di un file PostScript nel formato specifico della stampante si realizza per una stampante PCL3 ad esempio con:

```
gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn \
    -sDEVICE=deskjet -r300x300 \
    /usr/share/doc/packages/ghostscript/examples/colorcir.ps \
    quit.ps
```

A seconda del modello potete ripiegare anche su `cdjmomo`, `cdj500` o `cdj550` o sul driver alternativo `hpdj`:

```
gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn \
    -sDEVICE=hpdj -r300x300 \
    -sModel=500 -sColorMode=mono -dCompressionMethod=0 \
    /usr/share/doc/packages/ghostscript/examples/colorcir.ps \
    quit.ps
```

Ogni comando può essere immesso anche senza \, però in questo caso *in una singola riga*.

Conversione in ESC/P, ESC/P2 o matrice ESC/P

La conversione di un file PostScript in un formato di stampante ESC/P2, ESC/P o ESC/P a matrice si ha, ad esempio, con i comandi:

```
gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn \
    @stcany.upp \
    /usr/share/doc/packages/ghostscript/examples/colorcir.ps \
    quit.ps
```

```
gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn \
    -sDEVICE=stcolor -r360x360 \
    -dBitsPerPixel=1 -sDithering=gsmono -dnoWeave \
    -sOutputCode=plain \
    /usr/share/doc/packages/ghostscript/examples/colorcir.ps \
    quit.ps
```

Qui si vede la differenza tra l'immissione del comando nel caso in cui si usa un file per il driver `uniprint` e quando si usa un altro driver Ghostscript. Dal momento che tutti i parametri del driver si trovano nel file parametro uniprint, a differenza degli altri driver Ghostscript, non serve indicarne altri.

Stampa diretta

Dopo ogni comando di cui sopra i dati da stampare risiedono in `/tmp/out.prn`, che con il seguente comando di `root`, a questo punto possono essere inviati direttamente alla stampante (dunque senza spooler o filtro di stampante), se la stampante è collegata alla prima porta parallela `/dev/lp0`: `cat /tmp/out.prn >/dev/lp0`

Elaborazione di PostScript e PDF

Con Ghostscript si possono generare file PostScript e file PDF, convertire un formato nell'altro e unire file PostScript e file PDF anche in ordine sparso.

Conversione di Postscript in PDF:

```
gs -q -dNOPAUSE -dSAFER \
    -sOutputFile=/tmp/colorcir.pdf -sDEVICE=pdfwrite \
    /usr/share/doc/packages/ghostscript/examples/colorcir.ps \
    quit.ps
```

Conversione del file PDF appena generato `/tmp/colorcir.pdf` in Postscript:

```
gs -q -dNOPAUSE -dSAFER \
    -sOutputFile=/tmp/colorcir.ps -sDEVICE=pswrite \
    /tmp/colorcir.pdf quit.ps
```

Dopo la riconversione da PDF a PostScript il file `/tmp/colorcir.ps` non è più identico all'originale `/usr/share/doc/packages/ghostscript/examples/colorcir.ps`, ma comunque questo non dovrebbe incidere sul risultato del processo di stampa.

Generare un file PostScript e da file PostScript e PDF:

```
gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.ps \
    -sDEVICE=pswrite \
    /usr/share/doc/packages/ghostscript/examples/escher.ps \
    /tmp/colorcir.pdf quit.ps
```

Generare un file PDF da file PostScript e PDF:

```
gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.pdf \
    -sDEVICE=pdfwrite /tmp/out.ps \
    /usr/share/doc/packages/ghostscript/examples/golfer.ps \
    /tmp/colorcir.pdf quit.ps
```

Purtroppo la riuscita di questo processo dipende dai file interessati.

6.7 I principi di a2ps

Se desiderate stampare un file di testo ASCII con Ghostscript, dovrete prima convertirlo in PostScript, dal momento che Ghostscript si aspetta come input un file PostScript. A tal fine utilizzate il programma a2ps (`a2ps`). Dato che `a2ps` non viene installato di default, dovrete installarlo voi.a2ps è uno strumento potentissimo per generare da semplici testi stampe PostScript di ottima qualità. a2ps è un programma versatile con molte opzioni per la riga di comando. La documentazione principale si trova nella – quella completa nella pagina info di `a2ps`.

6.7.1 Stampa diretta di un file di testo con a2ps

Per convertire un file di testo in PostScript con `a2ps`, in modo che un foglio contenga due pagine ridotte, digitate il seguente comando:

```
a2ps -2 &#8211;&#8211;medium=A4dj &#8211;&#8211;output=/tmp/out.ps file di te
```

Ad esempio con:

```
gs -r60 /tmp/out.ps
```

potete visualizzare l'output di a2ps sull'interfaccia grafica ai fini di una verifica, laddove eventualmente nella finestra di terminale dalla quale avete invocato `gs` dovrete premere il tasto Invio per passare alla visualizzazione della pagine seguente (Ctrl + c per uscire).

L'output di a2ps può essere convertito nel formato specifico della stampante con:

```
gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn \
    <parametri driver> /tmp/out.ps quit.ps
```

laddove i ⟨*parametri driver*⟩ vanno immessi in base alla stampante secondo la sezione precedente.

Come `root` l'output di Ghostscript con:

```
cat /tmp/out.prn >/dev/lp0
```

può essere inviato direttamente alla stampante - dunque senza passare per spooler della stampante o filtro della stampante - se la stampante è connessa alla prima interfaccia parallela `/dev/lp0`.

6.8 Conversione PostScript con psutils

Ai fini della conversione, stampate da una applicazione in un file `/tmp/in.ps` e con `file /tmp/in.ps` potete verificare che sia stato generato effettivamente un file PostScript.

Programmi, per convertire dati PostScript, si trovano nel pacchetto `psutils`. Soprattutto il programma `pstops` consente tantissimo per quanto riguarda la conversione. Vedi la pagina di manuale pstops. Il pacchetto `psutils` non viene installato di default, dunque dovete installarlo.

I comandi riportati di seguito funzionano solo con file PostScript, creati in modo da consentire una conversione, cosa che di solito è possibile, ma a seconda degli applicativi con cui è stato creato il file PostScript, ciò non sempre è il caso.

6.8.1 psnup

Con `psnup -2 /tmp/in.ps /tmp/out.ps` si ha la conversione di `/tmp/in.ps` in `/tmp/out.ps` con due pagine rimpicciolite l'una accanto all'altra su un foglio. Visto che cresce la complessità del processo di stampa, quando si tratta di riprodurre più pagine di dimensioni ridotte su di un solo foglio, alcune stampanti PostScript con poca memoria integrata, possono fallire nel tentativo di stampare incarichi diventati troppo complessi.

6.8.2 pstops

Per personalizzare la dimensione e il posizionamento con pstops immettete:

```
pstops '1:0@0.8(2cm,3cm)' /tmp/in.ps /tmp/out.ps
```

In questo caso si ha un riduzione del fattore 0.8, ovvero una pagina A4 di ca 21x 30 cm viene ridotta a 17x24 cm; ne risulta un ulteriore margine a destra di ca. 4 cm e nella parte superiore di ca. 6 cm, ed inoltre il tutto viene spostato di 2 cm verso destra e di 3 cm verso l'alto, per avere tutti i margini di uguale dimensione.

Con questo comando pstops si riesce a ridimensionare di molto ed inoltre si avranno margini generosi, dunque si adatta particolarmente per quei applicativi che vogliono far rientrare tanto in una pagina - per cui al momento della stampa `/tmp/in.ps` non tutto avrebbe trovato posto su un foglio.

Un altro esempio:

```
pstops '1:0@0.8(2cm,3cm)' /tmp/in.ps /tmp/out1.ps
psnup -2 /tmp/out1.ps /tmp/out.ps
```

Con questo comando si hanno due pagine notevolmente ridimensionate, l'una accanto all'altra su un foglio – però con tanto spazio tra le due pagine ridimensionate. Si raggiungono miglior risultati se si posizionano le pagine singolarmente:

```
pstops '2:0L@0.6(20cm,2cm)+1L@0.6(20cm,15cm)' \
    /tmp/in.ps /tmp/out.ps
```

Il comando va immesso senza \ su una riga sola.

Ecco il risultato che produce `pstops '2:0L@0.6(20cm,2cm)+1L@0.6(20cm,15cm)'`:

2:0 ... +1 significa che 2 pagine vengono sovrapposte laddove le pagine modulo 2 vengono contate in modo alternato una volta come pagina 0 (modulo 2) e una come volta pagina 1 (modulo 2).

0L@0.6(20cm,2cm) significa, che la pagina 0 (modulo 2) viene girata per 90 gradi verso sinistra, scalata del fattore 0.6, e in seguito spostata di 20cm verso destra e di 2cm in alto.

1L@0.6(20cm,15cm) In modo anologo la pagina 1 (modulo 2) viene girata di 90 gradi verso sinistra, scalata del fattore 0.6, ed in seguito spostata di 20cm verso destra e di 15cm in alto.

In PostScript l'origine (il punto zero) di un sistema di coordinate è l'angolo in basso a sinistra del foglio, che qui viene contrasseganto con + (s. Abb. 6.1):

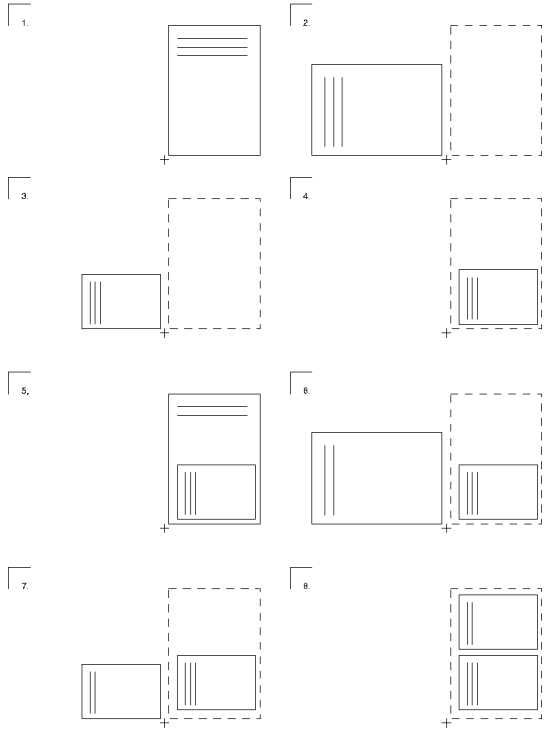

Figura 6.1: *Illustrazione dei singoli passaggi con pstops*

1. Ecco una pagina 0 (modulo 2) con tre righe di testo:
2. Dopo una rotazione verso sinistra di 90 gradi.
3. Dopo la riduzione del fattore 0.6.
4. Dopo lo spostamento di 20 cm verso destra e di 2 cm verso l'alto.

5. Sovrapposizione della pagina 1 (modulo 2) con due righe di testo.
6. Dopo la rotazione di 90 gradi verso sinistra della pagina 1 (modulo 2).
7. Dopo la riduzione del fattore 0.6 della pagina 1 (modulo 2).
8. Dopo lo spostamento della pagina 1 (modulo 2) di 20 cm verso destra e di 15 cm verso l'alto.

6.8.3 psselect

psselect vi permette di selezionare singole pagine. Con il comando `psselect -p2-5 /tmp/in.ps /tmp/out.ps` selezionate da `/tmp/in.ps` le pagine 2,3,4 e 5 emettendo le in `/tmp/out.ps`.Con `psselect -p-3 /tmp/in.ps /tmp/out.ps` selezionate tutte le pagine fino a alla pagina 3. Il comando `psselect -r -p4- /tmp/in.ps /tmp/out.ps` seleziona tutte le pagine a partire dalla pagina 4 fino all'ultima pagina e li emmetto nell'ordine inverso.

6.8.4 Verifica allo schermo con Ghostscript

Il file PostScript `/tmp/out.ps` si lascia visualizzare nella superficie grafica di Ghostscript con `gs -r60 /tmp/out.ps` pagina per pagina. Premendo il tasto invio nella finestra di terminale nella quale avete invocato Ghostscript, il file PostScript viene visualizzato pagina per pagina. Per chiudere, premete i tasti Ctrl+C.

Il programma `gv` del `gv` è un front-end grafico per Ghostscript. Viene richiamato nella superficie grafica con `gv /tmp/out.ps` e consente soprattutto una adeguata rappresentazione del formato orizzontale, dell'ingrandimento o del ridimensionamento (però non nel file PostScript in sé) e la selezione di singole pagine - soprattutto anche per stampare direttamente da `gv`.

6.9 La codificazione di testi ASCII

Ogni carattere di un semplice testo è rappresentato da una combinazione di numeri. In una tabella è riportato quale codice corrisponde a quale carattere. A seconda della tabella di codificazione la riproduzione della medesima sequenza di codice può differire tra quanto emesso allo schermo e da quanto emesso dalla stampante.

Con set di caratteri standard sono possibili solo codici da 0 fino a 255.I caratteri con i codici 0 fino a 127 sono i caratteri `ASCII` (in particolare le lettere, cifre e caratteri speciali non inclusi sono i caratteri speciali di una determinata lingua), che sono sempre identici.

I codici 128 fino a 255 sono riservati ai caratteri speciali di ogni lingua (e.g. gli umlaut tedeschi). Dato che vi sono molto più di 128 caratteri specifici di una lingua, i codici 128 fino a 255 non sono dappertutto uguali, ma a secondo della locazione geografica lo stesso codice viene utilizzato per i diversi caratteri specifici di una lingua.

`ISO-8859-1` (o `Latin 1`) è il sistema di codificazione per le lingue dell'Europa occidentale mentre `ISO-8859-2` (o `Latin 2`) è quello per le lingue dell'Europa centrale ed orientale. Quindi e.g. il codice 241 (ottale) secondo ISO-8859-1 è un punto esclamativo capovolto, mentre secondo ISO-8859-2 un'A maiuscola con l'ogonek. ISO-8859-15 e ISO-8859-1 sono quasi del tutto simili, con la differenza, ad esempio, che ISO-8859-15 contiene il simbolo dell'euro (codice 244).

6.9.1 Illustrazione

Tutti i comandi vanno inseriti su di un singolo rigo senza backslash (\) a *fine rigo*.

Create un file esempio di testo ASCII con:

```
echo -en "\rCode 241(octal): \
\241\r\nCode 244(octal): \244\r\f" >example
```

Visualizzazione allo schermo

Nell' interfaccia grafica aprite tre finestre di terminale con i seguenti tre comandi:

```
xterm -fn -*-*-*-*-*-*-14-*-*-*-*-*-iso8859-1 -title iso8859-1 &
xterm -fn -*-*-*-*-*-*-14-*-*-*-*-*-iso8859-15 -title iso8859-15 &
xterm -fn -*-*-*-*-*-*-14-*-*-*-*-*-iso8859-2 -title iso8859-2 &
```

Visualizzate In ogni finestra di terminale il file esempio con il comando `cat example`.

In iso8859-1 avrete: codice 241 come punto esclamativo capovolto (spagnolo) codice 244 come cerchio con uncino (simbolo di valuta)

In iso8859-15 avrete: codice 241 come punto esclamativo capovolto (spagnolo) codice 244 come simbolo dell'Euro

In iso8859-2 avrete: codice 241 come A maiuscola con virgoletta (l'ogonek) codice 244 come cerchio con uncino (simbolo di valuta)

A causa della codificazione stabilita non è possibile usare contemporaneamente tutti i caratteri speciali di diverse lingue. Così e.g. il simbolo dell'euro non può essere utilizzato assieme alla A con l'ogonek nello stesso testo.

Per ulteriori informazioni sulla corretta rappresentazione: Per iso8859-1: iso_8859-1. Periso8859-2: l' iso_8859-2. Periso8859-15: l' iso_8859-15.

Stampa

A seconda della codificazione impostata per una queue, i testi ASCII (ovvero del file `example`) vengono stampati come descritto negli esempi. La stampa di documenti approntati con sistemi di videoscrittura non ne viene influenzata, poiché questi sistemi inviano alla stampante dati in formato PostScript e non ASCII.

Stampando `example`, si otterrà la codificazione utilizzato nel sistema di stampa per il testo ASCII. Con `a2ps` è possibile convertire il file `example` in PostScript, e stabilire il sistema di codificazione:

```
a2ps -1 -X ISO-8859-1 -o example-ISO-8859-1.ps example
a2ps -1 -X ISO-8859-15 -o example-ISO-8859-15.ps example
a2ps -1 -X ISO-8859-2 -o example-ISO-8859-2.ps example
```

Se si stampano i file PostScript `example-ISO-8859-1.ps`, `example-ISO-8859-15.ps` ed `example-ISO-8859-2.ps`, allora si avrà il sistema di codificazione stabilito con `a2ps`.

Boot e boot manager

In questo capitolo, vi presenteremo diversi metodi di caricare un sistema installato. Per facilitarne la comprensione, approfondiremo innanzitutto alcuni dettagli tecnici del processo di boot. Passeremo quindi a descrivere il boot manager attuale GRUB.

7.1 Il processo di boot sul PC

Dopo aver acceso il computer, vengono inizializzati dal BIOS (ingl. *Basic Input Output System*) schermo e tastiera e viene eseguito il test della memoria principale; il computer fino a questo punto non dispone ancora 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*). Poiché a questo punto il primo hard disk e la sua geometria dovrebbero essere stati rilevati, si prosegue da lì con il caricamento del sistema operativo.

Per farlo, viene caricato in memoria dal primo hard disk il primo settore di dati fisico di 512 byte e lì viene controllato il programma situato all'inizio di questo settore. La sequenza delle istruzioni eseguite determina l'ulteriore decorso del processo di boot. I primi 512 byte sul primo hard disk vengono perciò anche chiamati *Master Boot Record*.

Fino a questo punto (caricamento dell'MBR) il processo di boot si svolge in modo identico su ogni PC, indipendentemente dal sistema operativo installato, e il computer dispone fin qui solo delle routine (driver) memorizzate nel BIOS per l'accesso alle periferiche.

7.1.1 Master Boot Record

La struttura dell'MBR è stabilita da una convenzione estesa a tutti i sistemi operativi. I primi 446 byte sono riservati ai codici del programma. I successivi 64 byte offrono lo spazio per la tabella delle partizioni contenente fino a 4 registrazioni; vedi la sezione 1.7 a pagina 24. Senza la tabella delle partizioni, non esistono neppure i file system, in altre parole il disco rigido è praticamente inutilizzabile. 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.

7.1.2 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 in principio vuoti (!). Perciò una partizione Linux *non si inizializza 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).

7.1.3 Eseguire il boot da DOS o Windows 95/98

Nell'MBR di DOS del primo hard disk la registrazione di una partizione è indicata come *attiva bootable*, il che significa che il sistema da caricare va cercato in quella sede. Per questo DOS deve essere installato assolutamente sul primo disco rigido. Il codice del programma di DOS nell'MBR è il primo livello del bootloader *first stage bootloader* e controlla se sulla partizione indicata esiste un settore di boot valido.

Se esiste, in questo settore di boot può venire inizializzato il codice come "secondo livello" del boot loader (ingl. *secondary stage loader*). Il codice carica ora i programmi di sistema e alla fine del processo appare l'usuale prompt di DOS o parte la superficie grafica di Windows.

Sotto DOS è possibile contrassegnare come attiva una sola partizione primaria. Di conseguenza il sistema DOS non può venire collocato su drive logici in una partizione estesa.

7.2 Concetti di boot

Il più semplice "concetto di boot", riguarda un computer con un solo sistema operativo; per questo caso abbiamo già descritto il decorso della fase di avvio. Questo processo vale anche per PC su cui gira solo Linux. Teoricamente allora si potrebbe rinunciare all'installazione del boot loader, però non sarebbe possibile passare al kernel dei parametri durante l'avvio tramite la riga di comando (con particolari preferenze riguardo al processo di boot, ulteriore informazioni sull'hardware etc.). Appena su un computer sono installati più di un sistema operativo, vi sono anche diversi modi di gestire il processo di boot:

Eseguire il boot di ulteriori sistemi da dischetto
: Un sistema operativo può venire caricato dall'hard disk; gli altri tramite un dischetto di avviamento dal lettore di dischetti.

- *Premessa:* deve esserci un dispositivo di lettura per i dischetti atto al boot.
- *Esempio:* installate Linux su un computer su cui gira già Windows e avviate Linux sempre da un dischetto di boot.
- *Vantaggio:* vi risparmiate l'installazione del boot loader.
- *Svantaggi:* Dovete porre *particolare* attenzione ad avere in serbo sempre un numero sufficente di dischetti di boot funzionanti, e l'avvio dura di più.
- A seconda dell'utilizzo che fate del vostro computer, può essere uno svantaggio o un vantaggio il fatto che Linux debba venire avviato da un dischetto di boot.

Eseguire il boot di ulteriori sistemi da un supporto di memoria USB Le informazioni necessarie al boot possono venir lette anche da un supporto di memoria USB.

Installazione di un boot manager Un boot manager permette di avere su un computer contemporaneamente più sistemi e di usarli alternativamente. 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. I boot manager di SUSE LINUX (LILO ed il suo successore GRUB) caricano 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.

7.3 File mappa, LILO e GRUB

La difficoltà principale durante l'avvio di un sistema operativo consiste nel fatto che il kernel è un file in un file system in una partizione su di un disco rigido. Per il BIOS, file system e partizioni sono concetti del tutto sconosciuti.

Per ovviare a questa difficoltà sono state introdotte "mappe" e "file mappa", in essi vengono annotati i blocchi fisici del disco rigido, occupati da file logici. Quando un file mappa viene elaborato, il BIOS carica i blocchi fisici nella sequenza indicata nei file mappa, e crea così il file logico nella memoria.

La differenza tra LILO e GRUB è che LILO si affida completamente a file mappa, mentre GRUB cerca di liberarsi dalle mappe, non appena gli è possibile durante il boot. Questo gli viene consentito dal *File System Code* che permette di accedere a file tramite l'indicazione del percorso e non solo attraverso i numeri di blocco.

Questa differenza ha dei motivi "storici". Agli inizi vi erano tanti file system Linux che cercavano di affermarsi. Werner Almesberger sviluppò un boot loader (LILO) a cui non serviva "sapere" su quale file system si trovasse il kernel da caricare. Le origini di GRUB risalgono ai tempi di Unix e BSD. Ognuno aveva scelto un file system e riservato al principio di esso un'area determinata per il boot loader che conosceva la struttura del file system, di cui era parte integrante, e trovava lì i kernel nella directory root.

Nota

Quando installare quale boot loader?

Se eseguite un aggiornamento da una vecchia versione di SUSE LINUX che utilizzava LILO, viene installato nuovamente LILO. Se eseguite una nuova installazione viene installato invece GRUB, almenoché la partizione root non venga installata su uno dei seguenti sistemi Raid:

- Controller Raid che dipendono dalla CPU (come p.es. tanti controller Promise oppure Highpoint)
- Software-Raid
- LVM

Dei dettagli riferiti alla installazione e configurazione di LILO sono reperibili nella banca dati di supporto; basta eseguire una ricerca immettendo come parola chiave "LILO" (`http://portal.suse.de/sdb/en/index.html`).

Nota

7.4 Boot con GRUB

GRUB (*Grand Unified Bootloader*) è composto come già LILO di 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 GRUB consiste nel caricare il secondo livello del boot loader.

Qui iniziano le differenze tra GRUB e LILO. stage2 (livello 2) accede ai file system. Al momento vengono supportati ext2, ext3, reiser FS, jfs, xfs, minix e il DOS FAT FS di Windows. GRUB è in grado di accedere a file system di dispositivi a disco Bios (dischetti o dischi rigidi rilevati dal BIOS) prima del boot, motivo per cui modifiche apportate al file di configurazione di GRUB 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.

GRUB presenta il vantaggio di poter modificare i parametri di boot *prima* del boot. Se per caso è stato commesso un errore editando il file menu in questo modo si potrà correre ai ripari. Inoltre potrete immettere i comandi di boot in maniera interattiva al prompt. Potrete inoltre caricare dei sistemi operativi non registrati nel menu di boot. GRUB offre la possibilità di rilevare la locazione del kernel e initrd prima ancora del boot.

7.4.1 Il menu di boot di GRUB

Lo splash screen grafico con il menu di boot viene configurato tramite il file di configurazione di GRUB`/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 YaST o il vostro editor preferito.

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 block notation per esempio:

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

I nomi dei dispositivi in GRUB vengono spiegati nella sezione 7.4.1. 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 trasmessi al kernel tramite la riga 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 ed di initrd. `root` ha come unico argomento un dispositivo GRUB oppure una partizione su un tale dispositivo. A tutti i percorsi del kernel, initrd o altri file senza una esplicita indicazione di un dispositivo viene preposto il dispositivo fino al prossimo comando `root`. Questo comando non è incluso in un `menu.lst` generato durante l'installazione.

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 7.4.1 a pagina 185.

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`). Il primo disco rigido è sempre `hd0`, il lettore del dischetto `fd0`.

Nota

Conteggio delle partizioni in GRUB

In GRUB il sistema di conteggio delle partizioni inizia da zero. (`hd0,0`) è la prima partizione del primo disco rigido; in un comune PC da scrivania con un disco come primary master il nome di dispositivo è `/dev/hda1`.

Nota

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
...
```

Nota

IDE, SCSI o RAID

GRUB non distingue tra dispositivi IDE, SCSI o RAID. Tutti i dischi rigidi rilevati dal BIOS o da altri controller, vengono conteggiati nella sequenza di boot preimpostata nel BIOS.

Nota

Il fatto che nomi di dispositivi Linux non si lasciano correlare in modo chiaro ai nomi di dispositivi BIOS si ha sia con LILO che con GRUB. Entrambi utilizzano degli algoritmi simili 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 7.4.2 a pagina 188.

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 GRUB 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 incide sullo splash screen, solo dopo esserne uscito 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, GRUB esegue il boot in modo automatico.

Il secondo blocco più esteso elenca i sistemi operativi da poter caricare.

- 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` controllate il caricamento e l'esecuzione del 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".

Nota

Cambiare la sequenza degli hard disk

Alcuni sistemi operativi (p.es. Windows) possono essere caricati solo dal primo hard disk. Se avete installato un sistema operativo di questo tipo su un hard disk che non sia il primo, potete modificare la sequenza di caricamento tramite le relative registrazioni di menu. Questo funziona solo se il sistema operativo all'avvio accede all'hard disk tramite il BIOS.

```
 ...
title windows
   map (hd0) (hd1)
   map (hd1) (hd0)
   chainloader(hd1,0)+1
...
```

Qui Windows deve essere avviato dal secondo hard disk. La sequenza degli hard disk può venir modificata tramite `map`. Tenete presente che questa modifica *non* incide sulla logica interna del file menu di GRUB e alla voce `chainloader` va indicato il secondo hard disk.

Nota

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.

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 LILO – potete immettere propri parametri di boot. GRUB va però ancora oltre. 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.

Nota

Mappatura della tastiera durante il boot

Tenete presente che al boot si ha la mappatura americana dei tasti e che di conseguenza i caratteri speciali sono scambiati.

Nota

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 (Enter) 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.

7.4.2 Il file device.map

Come già detto, 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 controllo 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/hdb
(hd2)  /dev/sda
(hd3)  /dev/sdb
```

Dato che la sequenza di hard disk IDE, SCSI ed altri tipi di hard disk 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 (vedi la sezione 7.4.3 a fronte). 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:

```
grub --batch --device-map=/boot/grub/device.map < /etc/grub.conf
```

7.4.3 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 opzioni richieste 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
```

Le singole registrazioni hanno il seguente significato:

root (hd0,4) Con questo comando si istruisce GRUB a riferirsi alla prima partizione logica del primo disco rigido, dove trova i suoi file di boot.

install `parametri` 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.

La GRUB shell

GRUB esiste in due versioni. Una volta come boot loader e una 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 salvataggio di un sistema difettoso.

Solo se la GRUB shell gira quale programma Linux (da invocare con `grub` come illustrato ad esempio nella sezione 7.4.2 nella pagina precedente), entra in gioco l'algoritmo di correlazione. Il programma legge il file `device.map`. Per maggiori dettagli vedi la sezione 7.4.2 a fronte.

7.4.4 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 - una volta caricato il sistema - solo root può accedervi. Impostando una password evitate che vi siano degli accessi di questo tipo durante la 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:

- Immettete al root prompt `grub`.
- Cifrate la password nella GRUB shell:

```
grub> md5crypt
Password: ****
Encrypted: $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

- 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 GRUB in fase di boot è protetta, solo dopo aver immesso (p) e la password sarà possibile eseguire dei comandi. Continua ad essere consentito agli utenti di lanciare un sistema operativo dal menu di boot.

- 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 (Enter) per giungere al menu ed in seguito (p) per ottenere un prompt per la password. Dopo aver immesso la password e premuto (Enter) viene caricato il sistema operativo selezionato in precedenza (in questo caso Linux).

Nota

Boot password e splash screen

Se utilizzate una boot password per GRUB il consueto splash screen non è più a vostra disposizione.

Nota

7.4.5 Difficoltà possibili e ulteriori informazioni

Nota

Difficoltà al boot con GRUB

In fase di avvio GRUB controlla la geometria dei dischi connessi. A volte il BIOS emette delle indicazioni non consistenti e GRUB comunica un GRUB Geom Error. (vedi a riguardo `http://portal.suse.com/sdb/en/2002/09/fhassel_grub_overview.html`). In questi casi utilizzate LILO o aggiornate eventualmente il BIOS. Informazioni dettagliate riguardanti all'installazione, configurazione e manutenzione di LILO sono reperibili nella banca dati di supporto di SUSE `http://portal.suse.de/sdb/en/2004/01/lilo_overview.html`.

Nota

Sul sito web: `http://www.gnu.org/software/grub/` trovate informazioni dettagliate su GRUB anche in inglese o se preferite in tedesco e giapponese. Il manuale in linea è comunque inglese.

Se avete installato texinfo nella shell immettendo `info grub` potete visualizzare 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'`http://portal.suse.de/sdb/de/index.html`, gli articoli sono tradotti tra l'altro anche in inglese.

7.5 Rimuovere il bootloader Linux

Vi sono due metodi per disinstallare il bootloader Linux:

- Ripristinate il backup dell'MBR originale tramite il modulo boot loader di YaST YaST crea automaticamente questo backup. Il modulo boot loader di YaST viene descritto nella parte dedicata alla installazione nel *Manuale dell'utente*.
- Installate un altro bootloader oppure ripristinate l'MBR di DOS/Windows.

Attenzione

Un backup del settore di boot non è valido se la partizione in questione ha ricevuto un nuovo file system. La tabella delle partizioni in un backup dell'MBR non è valida se nel frattempo l'hard disk in questione è stato partizionato in modo diverso; tali backup sono delle "bombe ad orologeria", la cosa migliore è cancellarli subito da `/boot/backup.mbr`!

Attenzione

7.5.1 Ripristinare MBR (DOS/Win9x/ME)

Un MBR di DOS o Windows si lascia ripristinare con il comando MS-DOS (disponibile dalla versione DOS 5.0) `fdisk /MBR` o sotto OS/2 con il comando `fdisk /newmbr`.

Questi comandi riscrivono solo i primi 446 byte (il codice di boot) nell'MBR e non vanno a toccare l'attuale tabella delle partizioni, almeno che l'MBR (vedi 7.1.1 a pagina 178) a causa del "numero magico" errato non venga riconosciuto: allora la tabella delle partizioni viene riempita di zeri! *Non dimenticate* di impostare con fdisk la partizione di avvio nuovamente come *attiva* (*bootable*); le MBR-routine di DOS, Windows, OS/2 lo richiedono!

7.5.2 Ripristinare l'MBR (Windows XP)

Eseguite il boot dal CD di Windows XP, premete durante la configurazione il tasto Ⓡ per avviare la console di ripristino. Selezionate dall'elenco il vostro Windows XP ed immettete la password per l'amministratore. Al prompt, immettete `FIXMBR` e confermate la domanda riguardante la sicurezza con `y`. Con `exit` potete riavviare il computer.

7.5.3 Ripristinare l'MBR (Windows 2000)

Eseguite il boot dal CD di Windows 2000, premete durante la configurazione il tasto Ⓡ ed in seguito il tasto Ⓚ nel menu successivo per avviare la console di ripristino. Selezionate dall'elenco il vostro Windows 2000 ed immettete la password per l'amministratore. Al prompt, immettete `FIXMBR` e confermate la domanda di sicurezza con `y`. Con `exit` potete riavviare il computer.

7.6 Per andare sul sicuro: creare il CD di avvio

Se doveste incontrare delle difficoltà ad eseguire il boot del vostro sistema installato tramite un bootmanager, o non volete/potete installare Lilo o Grub nell' MBR del vostro disco rigido, e disponete di un masterizzatore potete creare un CD di avvio su cui masterizzare i file di avvio di Linux.

7.6.1 CD di avvio con ISOLINUX

Il modo più semplice consiste nell'utilizzare il bootmanager Isolinux. Anche per i CD di installazione di SuSE è stato usato Isolinux, per renderle avviabili.

- Eseguite il boot del vostro sistema installato seguendo questo procedimento: inserite il CD/DVD di installazione ed eseguite il boot come nel caso di una normale installazione. Nel menu di boot selezionate l'opzione 'Installazione' e nel prossimo menu selezionate la voce 'Avvio del sistema installato'. La partizione root viene rilevata automaticamente e avviato il sistema.
- Installate con YaST il pacchetto `syslinux`.
- Aprite una root-shell. Con i seguenti comandi viene generata una directory temporanea per il CD di avvio e vi vengono copiati i file necessari per il boot di un sistema Linux (il bootloader Isolinux, il kernel ed initrd).

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

- Con il vostro editor preferito generate ora il file di configurazione del bootloader `/tmp/CDroot/isolinux.cfg`. Inserite il seguente contenuto:

  ```
  DEFAULT linux
  LABEL linux
    KERNEL linux
    APPEND initrd=initrd root=/dev/hdXY [parametro di boot]
  ```

Per il parametro `root=/dev/hdXY` inserite la vostra partizione root. Se non siete sicuri sulla denominazione della partizione consultate semplicemente il file `/etc/fstab`. Per il valore `[parametro di boot]` potete aggiungere delle opzioni aggiuntive da usare in fase di boot. Il file di configurazione potrebbe assumere per esempio questo aspetto:

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

- In seguito con il comando riportato sotto viene generato dai file un file system ISO9660 per il CD (il comando va scritto in una sola riga):

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

- Ora potete masterizzare il file `/tmp/bootcd.iso` su CD, con K3b o semplicemente immettendo sulla riga di comando: `cdrecord -v -eject speed=2 dev=0,0,0 /tmp/bootcd.iso`.

  Eventualmente va adattato il parametro `dev=0,0,0` all'ID SCSI del masterizzatore (che vi viene indicato con il comando `cdrecord -scanbus`, cfr. anche la pagina di manuale con `man cdrecord`).

- Adesso provate il vostro CD di avvio! Riavviate il computer e verificate se il vostro sistema Linux si avvia correttamente dal CD.

Lavorare coi notebook

Questo capitolo tratta delle particolarità dell'utilizzo di dispositivi portatili — in particolare dei laptop — sotto Linux. Verrà illustrato come configurare schede da PC (PCMCIA) e configurare diversi profili di sistema tramite SCPM e la comunicazione wireless tramite IrDA e Bluetooth.

8.1 PCMCIA

PCMCIA sta per *Personal Computer Memory Card International Association* ed indica hardware e software in relazione con questa associazione.

8.1.1 L'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, sono nella maggior parte dei casi convenienti e di norma vengono supportate senza creare problemi.

Schede CardBus si tratta è uno standard più recente. Viene utilizzato un bus a 32 bit, sono di conseguenza più veloci ma anche più cari. Dato che la velocità di trasmissione viene limitata in altri punti, nella maggioranza dei casi non conviene sobbarcarsi in lavoro aggiuntivo. Per queste schede vi sono numerosi driver che a volte però risultano essere poco stabili – ciò dipende anche dal controller PCMCIA.

Quale scheda è inserita, viene indicato – con il servizio PCMCIA attivo – dal comando `cardctl ident`. 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/CardBus-Bridge che crea la connessione tra la scheda e PCI-Bus e nei dispositivi più datati anche la connessione all'ISA-Bus. Questi controller sono quasi sempre compatibili con il chip di Inteli82365. Vengono supportati tutti i comuni modelli. Il tipo di controller si lascia stabilire anche con il comando `pcic_probe`. Se si tratta di un dispositivo PCI, il comando `lspci -vt` fornisce ulteriori informazione.

8.1.2 Il software

Differenze tra i due sistemi PCMCIA esistenti

Attualmente vi sono due sistemi PCMCIA: PCMCIA esterno e PCMCIA kernel. Il sistema PCMCIA esterno di David Hinds è il più vecchio dei due e così anche quello maggiormente collaudato e si continua a svilupparlo

ancor oggi. I sorgenti dei moduli utilizzati non sono integrati nei sorgenti del kernel, per questo il nome di sistema "esterno". A partire dal kernel 2.4 vi sono moduli alternativi nei sorgenti kernel che costituiscono il sistema PCMCIA del kernel ("Kernel-PCMCIA"). I moduli di base sono stati compilati da Linus Torvalds e sono indicati soprattutto per il supporto di CardBus bridge più recenti.

Purtroppo i due sistemi sono incompatibili. Inoltre i due sistemi hanno un set diverso di driver per schede. Così in base all'hardware che utilizzate potete scegliere solo uno dei due sistemi. Il default di SUSE LINUX è il più recente PCMCIA kernel. Comunque sussiste la possibilità di cambiare sistema. Per fare ciò nel file `/etc/sysconfig/pcmcia` alla variabile `PCMCIA_SYSTEM` va assegnato il valore `external` o `kernel` e bisogna riavviare PCMCIA con `rcpcmcia [re]start external,kernel`. Per maggiori dettagli consultate `/usr/share/doc/packages/pcmcia/README.SuSE` (in inglese)

I moduli di base

I moduli kernel per entrambi i sistemi risiedono nei pacchetti kernel. Sono necessari inoltre i pacchetti `pcmcia` e `hotplug`.

All'avvio di PCMCIA vengono caricati i moduli `pcmcia_core`, `i82365` (PCMCIA esterno) o `yenta_socket` (PCMCIA kernel) e `ds`.

Raramente al posto di `i82365` o `yenta_socket` viene richiesto il modulo `tcic` che inizializzano il controller PCMCIA e mettono a disposizione le funzionalità di base.

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 a seconda del sistema PCMCIA selezionato e dell'hardware utilizzato dal gestore di scheda (ingl. card manager) o dal sistema hotplug del kernel. Nel caso di PCMCIA esterno entra in gioco solo il gestore della scheda. Con il PCMCIA kernel il gestore della scheda controlla solo schede PC, mentre le schede CardBus vengono controllate dall'hotplug. Il gestore della scheda viene lanciato dallo script di avvio della PCMCIA dopo l'avvenuto caricamento dei moduli di base. Visto che l'hotplug oltre alla PCMCIA controlla anche altri sottosistemi esiste per questa funzione uno script di avvio proprio.

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 azioni a seconda dell'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.

Sia l'avvio di PCMCIA che gli eventi della scheda sono protocollati nel file 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 dei problemi. Questo funziona bene 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 `cardctl eject`.

Con questo comando disattivate tutte le schede del notebook. Per disattivare solo una delle schede, indicate in aggiunta il numero dello slot, p.es. `cardctl eject 0`.

8.1.3 La configurazione

Attraverso il runlevel editor di YaST oppure con `chkconfig` dalla riga di comando potete determinare se avviare PCMCIA o l'hotplug al boot.

In `/etc/sysconfig/pcmcia` vi sono quattro variabili:

`PCMCIA_SYSTEM` determina, quale sistema di PCMCIA viene utilizzato.

`PCMCIA_PCIC` contiene il nome del modulo che indirizza 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`.

PCMCIA_PCIC_OPTS accetta dei parametri per il modulo `i82365`. vd. la pagina di manuale di `i82365`. Se utilizzate `yenta_socket`, queste opzioni vengono ignorate, poiché `yenta_socket` non ha opzioni.

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` trovate i dettagli sulla sintassi di questi file.

Schede di rete (Ethernet, Wireless LAN e TokenRing)

Queste schede 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 nel capitolo 14.4 a pagina 335. Leggete attentamente le indicazioni di schede atti all'hotplug.

ISDN

Anche con schede PC ISDN la configurazione avviene per sommi capi come per le altre schede ISDN con 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 si deve badare che la modalità di funzionamento sia sempre `hotplug`, e non `onboot`.

Anche le schede PCMCIA hanno dei cosiddetti modem ISDN. Sono schede modem o multifunzione con un kit di connessione ISDN aggiuntivo e vanno trattati alla stregua di un modem.

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 per schede PCMCIA ci sono dei cosiddetti softmodem. Generalmente non sono supportati. Se esistono dei driver, vanno integrati nel sistema.

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 ad essa 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 presenti.

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.

Attenzione

Prima di prelevare una scheda SCSI o IDE, le partizione dei dispositivi ad essa collegati devono essere smontate (ingl. unmount). Se si dimentica di farlo, si potrà accedere a questi dispositivi solo dopo un riavvio del sistema, anche se il resto del sistema continua a girare stabilmente.

Attenzione

Potete installare Linux anche completamente su dischi esterni, che però renderà più complesso il procedimento di avvio. Ad ogni modo serve un bootdisk che contiene il kernel ed una init-ramdisk (initrd) per ulteriori informazioni si veda la sezione 12.3 a pagina 273.

`initrd` contiene un file system virtuale, con tutti i moduli e programmi PCMCIA necessari. Il bootdisk o le immagini del bootdisk sono strutturate nello stesso modo, così avete la possibilità di avviare sempre una installazione esterna. Si tratta comunque di un procedimento poco comodo dover caricare manualmente il supporto PCMCIA. Gli utenti più esperti possono crearsi un dischetto per l'avvio su misura per il sistema in questione. Il PCMCIA-HOWTO in lingua inglese vi fornisce delle indicazioni a riguardo nella sezione *5.3 Booting from a PCMCIA device*.

8.1.4 Problemi

Finora utilizzare PCMCIA su alcuni notebook o con alcune schede causava dei problemi. La maggior parte delle difficoltà si lasciano risolvere facilmente, premesso che si affronta il problema in modo sistematico.

Attenzione

Visto che SUSE LINUX offre sia PCMCIA esterno che kernel, durante il caricamento manuale di moduli bisogna considerare una particolarità. I due sistemi PCMCIA utilizzano moduli omonimi che risiedono in diverse sottodirectory sotto `/lib/modules/<versionedelkernel/`. Queste sottodirectory si chiamano `pcmcia` per PCMCIA kernel e `pcmcia-external/` per PCMCIA esterno. Per questo motivo deve essere indicata la sottodirectory durante il caricamento manuale dei moduli:

```
modprobe -t <sottodirectory> <nome_del_modulo>
```

Attenzione

Innanzitutto si deve stabilire se il problema è da ricondurre alla scheda, o se il problema è causato dal 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 informativi vengono protocollati in `/var/log/messages/`. Per questo il file va osservato con `tail -f /var/log/messages` durante i test necessari. Così le possibili cause di errore - descritte di seguito - si lasciano ridurre a due.

Non funziona il sistema di base PCMCIA

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.

A tal fine sono richiesti i comandi (da dare come utente `root`):

```
modprobe -t <dir> pcmcia_core
modprobe -t pcmcia-external i82365
```

per PCMCIA esterno

```
modprobe -t pcmcia yenta_socket
```

o per PCMCIA kernel

o – in casi rarissimi – `modprobe -t <dir> tcic` e

```
modprobe -t <dir> ds
```

I moduli critici sono i primi due.

Se l'errore si verifica durante il caricamento di `pcmcia_core`, potete trovare utili indicazioni nella pagina di manuale su `pcmcia_core`. Le opzioni ivi descritte possono essere testate con il comando modprobe. Come esempio disabiltiamo il supporto APM dei moduli PCMCIA che a volte causa delle difficoltà. In questi casi usate l'opzione `doapm` con `do_apm=0` viene disattivato il power management:

```
modprobe -t <dir> pcmciacore do_apm=0
```

Se l'opzione selezionata conduce al successo, essa viene scritta nel file `/etc/sysconfig/pcmcia` accanto alla variabile `PCMCIA_CORE_OPTS`:

```
PCMCIA_CORE_OPTS="do_apm=0"
```

Vi sono dei casi in cui esaminare settori IO liberi crea delle difficoltà a causa di componenti di hardware. Questo incoveniente si lascia evitare con `probe_io=0`. Se volete utilizzare più opzioni, lasciate uno spazio tra di loro:

```
PCMCIA_CORE_OPTS=do_apm=0 probe_io=0
```

Se durante il caricamento del modulo `i82365` si verificano degli errori, consultate la pagina di manuale di `i82365`.

Il problema in questi casi è dovuto ad un conflitto di risorse, un interrupt, una porta IO o l'area della memoria è già occupata. Il modulo `i82365` controlla queste risorse prima di renderle disponibili per una scheda, a volte però proprio questo controllo è la causa del problema. Infatti il controllo dell'interrupt 12 (dispositivi PS/2) comporta un blocco del mouse e/o tastiera. In questi casi è d'aiuto il parametro `irq_list=<elenco_degli_IRQs>`. L'elenco deve contenere tutti gli IRQ che possono essere utilizzati. Dunque `modprobe i82365 irq_list=5,7,9,10` o in modo permanente in `/etc/sysconfig/pcmcia`.

```
PCMCIA_PCIC_OPTS="irq_list=5,7,9,10"
```

Inoltre vi è `/etc/pcmcia/config` e `/etc/pcmcia/config.opts`. Questi file vengono analizzati dal gestore delle schede. Le impostazioni ivi fatte diventano rilevanti solo per il caricamento dei moduli driver per le schede PCMCIA.

In `/etc/pcmcia/config.opts` potete includere o escludere anche IRQ, porte IO e aree della memoria. La differenza rispetto all'opzione`irqlist` è che le risorse escluse nel file `config.opts` non vengono utilizzate per una scheda PCMCIA, ma che comunque vengono controllate dal modulo di base `i82365`.

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 tenere in considerazione se la scheda viene amministrata dal gestore di schede o dall'hotplug. Ricordatevi: con PCMCIA esterno entra in gioco sempre il gestore di schede, con PCMCIA kernel il gestore di schede amministra schede PC-Card, e l' hotplug le schede CardBUS. Qui viene trattato solo il gestore di schede.

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 di schede non riesce ad attribuire alcun driver alla scheda. Per poter attribuire un driver si ricorre a `/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 l'id della scheda. Ulteriori informazioni nel PCMCIA-HOWTO (sezione 6) e nella pagina di manuale di `pcmcia`. Dopo aver modificato `/etc/pcmcia/config` o `/etc/pcmcia/*.conf` bisogna ricaricare la correlazione dei driver; basta un `rcpcmcia reload`.

Il driver non viene caricato Una possibile causa è che nella banca dati dei driver è memorizzata una allocazione errata che per esempio può essere dovuto 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 (o addirittura iniziano a funzionare) che il 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.

Un'altra causa è un conflitto di risorse. Nella maggioranza delle schede PCMCIA non è rilevante con quale IRQ, porta IO oppure area di memoria vengano utilizzate, ma vi sono anche delle eccezioni. Allora dovreste testare le schede singolarmente ed eventualmente spegnere temporaneamente anche altri componenti di sistema come scheda audio, IrDA, modem o stampante. L'allocazione delle risorse del sistema può essere visualizzata con `lsdev`(e' del tutto normale che diversi dispositivi PCI utilizzano lo stesso IRQ).

Un modo per risolvere il problema sarebbe quello di usare una opzione adatta per il modulo `i82365`, (vedi sopra `PCMCIA_PCIC_OPTS`). Esistono delle opzioni anche per alcuni moduli di driver di schede che potete scoprire con `modinfo /lib/modules/<directory_PCMCIA_corretta>/<driver>.o` (serve il percorso completo per indirizzare il driver dal sistema PCMCIA corretto). 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 in pcmcia. Per testare le opzioni potete scaricare i driver di schede anche manualmente. Dovete solo fare attenzione ad utilizzare il modulo del sistema PCMCIA effettivamente in uso. Vedi l'avvertimento di sopra.

Una volta trovata la soluzione in `/etc/pcmcia/config.opts` può essere 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
```

Un problema che a volte si verifica con schede di rete di 10/100 MBit: il tipo di trasmissione non viene riconosciuto automaticamente. Qui si rivela utile il comando `ifport` o `mii_tool` con il quale si lascia visualizzare e modificare il tipo di trasmissione stabilito. Per eseguire automaticamente questi comandi, si deve adattare individualmente lo script `/etc/pcmcia/network`.

L'interfaccia non è stata configurata correttamente

In questo caso si consiglia di controllare ancora una volta la configurazione dell'interfaccia per escludere rari errori di configurazione. Con schede di rete si può inoltre aumentare

la velocità di trasmissione degli script di rete, assegnando in `/etc/sysconfig/network/config` alla variabile `DEBUG` il valore `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 (vedi `/var/log/messages`) la riga `set -x`. 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.

8.1.5 Installazione via PCMCIA

In alcuni casi il PCMCIA serve già ai fini dell'installazione, se si vuole installare attraverso la rete, oppure se il CD-ROM viene utilizzato tramite PCMCIA. A tal fine serve un dischetto di avviamento ed inoltre uno dei dischetti dei moduli.

Dopo il boot dal dischetto (oppure dopo aver selezionato 'Installazione manuale' al boot dal CD) viene inizializzato il programma linuxrc. Lì sotto la voce di menu 'Moduli del kernel (driver di hardware)' deve essere selezionata la voce 'Carica moduli PCMCIA'. Dapprima appaiono due campi di immissione dove poter immettere le opzioni per i moduli `pcmcia_core` e `i82365`. Di solito questi campi però rimangono vuoti. Le pagine di manuale per `pcmcia_core` e `i82365` risiedono sotto forma di file di testo sul primo CD nella directory `docu/`.

In SUSE LINUX viene installato il sistema PCMCIA esterno. Durante il processo di installazione i messaggi del sistema vengono emessi su diverse console virtuali, a cui potete accedere con (Alt) + (Tasto funzione).

Quando l'interfaccia grafica è attivata, si deve utilizzare una combinazione di (Ctrl), + (Alt),+ (Tasto funzione).

Già durante l'installazione vi sono dei terminali su cui possono essere eseguiti dei comandi. Finché gira linuxrc vi è la console 9 (una shell un pò spartana); appena il sistema di installazione è caricato (YaST è stato inizializzato) sulla console 2 trovate bash e tanti comuni strumenti di sistema.

Se durante l'installazione viene caricato un modulo driver errato per la scheda PCMCIA, il dischetto di avviamento deve venir adattato a mano, per cui dovete disporre di una buona conoscenza di Linux. Conclusa la prima parte della installazione, il sistema viene riavviato parzialmemte o completamente. Accade a volte che avviando PCMCIA il sistema si blocchi. A questo punto l'installazione si trova comunque in uno stato così avanzato che con l'opzione di boot `NOPCMCIA=yes`, Linux può essere avviato senza

PCMCIA, almeno nella modalità testo. Leggete la sezione 8.1.4 a pagina 200 per i dettagli. Eventualmente già dopo la prima parte del procedimento di installazione sarà possibile modificare delle impostazioni di sistema su console 2, per garantire la riuscita del riavvio.

8.1.6 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 delle determinate operazioni. Nel file `cardctl` trovate ulteriori dettagli, o immettendo `cardctl` otterrete un elenco di comandi validi.

Per questo comando vi è un frontend grafico cardinfo, con cui controllare le funzioni principali. Comunque `pcmcia-cardinfo` deve essere installato.

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`.

8.1.7 Aggiornare il kernel o il pacchetto PCMCIA

Se volete aggiornare il kernel, utilizzate i pacchetti kernel messi a disposizione da SUSE. Se dovesse essere necessario compilare un kernel proprio, allora vanno ricompilati anche i moduli PCMCIA. Durante la ricompilazione deve girare il kernel corretto, dato che dovrà fornire alcune informazioni. Il pacchetto `pcmcia` dovrebbe essere già installato, ma non inizializzato; in caso di dubbio eseguire ancora una volta `rcpcmcia stop`. Quindi si installa il pacchetto sorgente PCMCIA e si immette di seguito:

```
rpm -ba /usr/src/packages/SPECS/pcmcia.spec
```

Sotto `/usr/src/packages/RPMS/` troverete in seguito i nuovi pacchetti. Il pacchetto `pcmcia-modules` contiene i moduli PCMCIA per PCMCIA esterno. Questo pacchetto deve essere installato con `rpm --force`, poiché i file modulo appartengono ufficialmente al pacchetto kernel.

8.1.8 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 diversi articoli dedicati a questo tema; eseguite ad es. una ricerca con il lemma *Laptop* al seguente indirizzo `http://portal.suse.de/sdb/en/index.html`.

8.2 SCPM – System Configuration Profile Management

A volte si rende necessario - per ragioni diverse- modificare la configurazione di un computer. Il caso più frequente sarà di certo quello di un portatile utilizzato in ambienti di lavoro diversi, oppure perché per un determinato periodo si utilizza una differente componente di hardware, o anche perché si vuole semplicemente provare qualcosa. In ogni caso, ritornare allo stato originario del sistema non dovrebbe essere accompagnato da problemi o addirittura preferibilmente, dovrebbe essere possibile eseguire la riconfigurazione senza difficoltà alcuna.

Questo problema veniva risolto finora egregiamente solo per l'hardware PCMCIA, ove era possibile avere degli schemi che contenevano diverse configurazioni. Sulla base di tale principio abbiamo sviluppato SCPM (ingl. *System Configuration Profile Management*) che non si limita solo a componenti PCMCIA. Con l' SCPM potete scegliere liberamente una parte della configurazione del sistema di cui i diversi stati vengono riprodotti in propri profili di configurazione, o detto in altre parole: è come fare una istantanea della configurazione del sistema riproducibile in ogni momento. E la parte della configurazione la scegliete voi.

La configurazione di rete dei portatili sarà probabilmente l'ambito di applicazione principale del gestore dei profili della configurazione di sistema. Comunque c'è da considerare che diverse impostazioni di rete influiscono anche su altri elementi come ad es. sulle impostazioni per e-Mail o proxy, o ancora si devono considerare stampanti diverse a casa e in ufficio, la configurazione XFree per il beamer, particolari impostazioni per il risparmio energetico durante gli spostamenti, o un diverso fuso orario nelle filiali all'estero.

Visti i tanti scenari di applicazione sono innumerevoli le richieste cui deve adempiere questo strumento. Se avete delle proposte o delle critiche da fare su SCPM, contattateci, ci interessa molto il vostro feedback. Abbiamo

cercato di porre SCPM su di una struttura di base flessibile così da permettere p.es.anche una gestione dei profili basata su server. Se avete delle proposte o rilevato degli errori contattateci attraverso il nostro web front-end `http://www.suse.de/feedback` (preferibilmente in inglese).

8.2.1 Terminologia e principi

Ecco la terminologia usata di seguito per descrivere SCPM usata anche nella documentazione e nel modulo di YaST.

- *Configurazione del sistema* riguarda le principali impostazioni p.es. l'uso di partizioni del disco rigido o impostazioni della rete, scelta del fuso orario o impostazione 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 non significa che la configurazione del sistema attuale corrisponda esattamente al profilo, poiché la configurazione si lascia modificare in ogni momento.
- *Risorsa*: in relazione all'SCPM le risorse sono tutti quei elementi che contribuiscono alla configurazione del sistema; può essere un file o un soft link inclusi 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 che contengono un servizio ed i 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 attiviati che per la maggioranza dei casi dovrebbe rilevarsi sufficiente.

8.2.2 Modulo YaST per SCPM e ulteriore documentazione

Quale front-end grafico per SCPM (il pacchetto `scpm`) vi è un modulo di YaST (il pacchetto `yast2-profile-manager` da poter usare come alter-

nativa al front-end basato sulla riga di comando. Dato che le funzionalità dei due front-end non differiscono più di tanto e che conoscere il front-end basato sulla riga di comando può rilevarsi utile in diversi occasioni, sarà a quest'ultimo che dedicheremo questa sezione. Il modulo di YaST per SCPM è accompagnato da testi di aiuto che spiegano l'utilizzo del modulo. Le poche particolarità del modulo di YaST verranno trattate al momento opportuno.

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 tecnica per coloro che vogliono sperimentare con SCPM si trova sotto `/usr/share/doc/packages/scpm/`. Il comando `scpm` senza ulteriori argomenti elenca i vari comandi.

8.2.3 Configurare SCPM

Prima di iniziare a lavorare con SCPM bisogna abilitarlo. Di solito SCPM viene utilizzato per impostazioni di rete e di stampa, la configurazione di XFree86 e per alcuni servizi di rete. 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`. Potete abilitare o disabilitare i gruppi tramite `scpm activate_group NOME` oppure `scpm deactivate_group NOME`, laddove `NOME` va sostituito con il relativo nome del gruppo. I gruppi di risorsa si lasciano configurare comodamente anche tramite il rispettivo modulo di YaST.

Con `scpm enable` si abilita SCPM, la prima volta possono volerci alcuni istanti prima che venga inizializzato SCPM. Con `scpm disable` potete disabilitare SCPM in qualsiasi momento per evitare involontari passaggi da un profilo all'altro. Successivamente potrete semplicemente riabilitarlo.

8.2.4 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 ora anche il profilo attivo. `scpm active` ve lo mostrerà. Il profilo `default` è stato concepito come configurazione di base da

cui derivare gli altri profili. Per questo eseguite innanzitutto le impostazioni che devono essere applicate in modo uniforme a tutti i profili. Con `scpm reload` queste modifiche verranno memorizzate nel profilo attivo. Il profilo `default` può essere utilizzato, rinominato o cancellato a piacere.

Esistono due possibilità per aggiungere un nuovo profilo. Se il nuovo profilo (diciamo `work`) deve basarsi p.e. sul profilo `default`, immettete `scpm copy default work`. Con `scpm switch work` entrate nel nuovo profilo per configurarlo. A volte capita che la configurazione del sistema è stata modificata per determinati motivi e si vuole generare un profilo con questa configurazione. In questi casi immettete `scpm add work`. Adesso la configurazione attuale del sistema è salvata nel profilo `work` e il nuovo profilo è marcato come attivo; cioè con `scpm reload` salvate le modifiche nel profilo `work`.

I profili possono essere rinominati o cancellati con i comandi `scpm rename x y` e `scpm delete x`. Per rinominare p.es. `work` in `lavoro` e per cancellarlo di seguito, immettete `scpm rename work lavoro` e quindi `scpm delete lavoro`. Solo il profilo attivo non può essere cancellato.

Riassumendo i singoli comandi:

`scpm list` elenca tutti i profili disponibili

`scpm active` mostra il profilo attivo

`scpm add <nome>` salva l'attuale configurazione del sistema in un nuovo profilo e lo rendo quello attivo

`scpm copy <nome> <nuovonome>`
copia un profilo

`scpm rename <nome> <nuovonome>`
rinomina un profilo

`scpm delete <nome>` cancella un profilo

Indicazione relativa al modulo di YaST: esiste solo il bottone 'Aggiungi'. Apparirà di seguito la domanda se volete copiare un profilo esistente o se volete salvare la configurazione del sistema attuale. Per rinominare un profilo utilizzate 'Modifica'.

8.2.5 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. Potete entrare nel profilo attualmente attivo per salvare le modifiche apportate alle impostazioni della configurazione del sistema. Un'altra possibilità è rappresentata dal comando `scpm reload`.

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 anche dal profilo ancora attivo. In caso affermativo – come era il caso per le precedenti versioni di SCPM – è consigliabile farsi mostrare le singole risorse ed invocare il comando swtich, che esegue il passaggio, con il parametro `-r`, ovvero: `scpm switch -r work`.

In seguito SCPM confronta la configurazione del sistema attuale con il nuovo profilo a cui si passerà. Viene stabilito quali servizi di sistema devono essere fermati o riavviati 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 ció interessa solamente una piccola parte del sistema mentre la parte rimanente del sistema continua a funzionare in modo immutato.

Solo a questo punto vengono

1. fermati i servizi di sistema,
2. salvate tutte le risorse modificate (p.es. file di configurazione),
3. (ri)avviati i servizi del sistema.

8.2.6 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 `scpm set description "testo" work`

Può verificarsi il caso che durante il passaggio da un profilo all'altro debbano essere eseguite delle azioni aggiuntive non (ancora) previste dall' 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 ad un 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

Ecco il passaggio dal profilo `work` al profilo `home`:

1. Viene eseguito il prestop del profilo `work`.
2. Arresto dei servizi
3. Viene eseguito il poststop del profilo `work`.
4. Modifica della configurazione del sistema
5. Viene eseguito il prestart del profilo `home`.
6. Avvio dei servizi
7. Viene eseguito il poststart del profilo `home`.

Queste azioni possono essere eseguite con il comando `set`, cio è con `scpm set prestop <nomefile>`, `scpm set poststop <nomefile>`, `scpm set prestart <nomefile>` o `scpm set poststart <nomefile>`. Si deve trattare di un programma eseguibile, cioè gli script devono contenere il giusto interpreter (interprete) ed essere eseguibili almeno per il superutente (`root`).

Attenzione

Visto che questi script o programmi vengono eseguiti con i permessi del superutente non dovrebbero essere accessibili per un utente qualsiasi. Poiché gli script possono contenere informazioni riservate, si consiglia di permettere l'accesso in lettura al solo superutente. Impostate i permessi di questi programmi nel seguente modo `-rwx---- root root`.

```
chmod 700 <nomefile>
chown root.root <nomefile>
```

Attenzione

Tutte le altre impostazioni che sono state immesse con `set`, si possono visualizzare con `get`. Per esempio `scpm get poststart` fornisce il nome del programma poststart o nessun informazione se non è stato eseguito alcunché. Potete cancellare queste impostazioni sovrascrivendole con `""`; ad esempio `scpm set prestop ""`.

Come nel caso delle descrizioni tutti i comandi `set` e `get` possono essere applicati per un profilo qualsiasi. Basta aggiungere il nome del profilo. Per esempio `scpm get prestop <nomefile> work` o `scpm get prestop work`.

8.2.7 Scelta del profilo al boot

Sussiste la possibilità di scegliere il profilo prima del boot. Basta immettere il parametro di boot `PROFILE=<nomeprofilo>` al prompt di boot.

Anche nella configurazione del boot loader (`/boot/grub/menu.lst`) si utilizza il nome del profilo per l'opzione `title`. GRUB è il bootloader di default. Una descrizione dettagliata si trova nella sezione 7.4 a pagina 181; oppure immettete `info grub`. La configurazione di GRUB sarà p.es.:

Exempio 8.1: *Il file /boot/grub/menu.lst*

```
gfxmenu (hd0,5)/boot/message
color white/green black/light-gray
default 0
timeout 8

title work
   kernel (hd0,5)/boot/vmlinuz root=/dev/hda6 PROFILE=work
   initrd (hd0,5)/boot/initrd

title home
   kernel (hd0,5)/boot/vmlinuz root=/dev/hda6 PROFILE=home
   initrd (hd0,5)/boot/initrd

title road
   kernel (hd0,5)/boot/vmlinuz root=/dev/hda6 PROFILE=road
   initrd (hd0,5)/boot/initrd
```

Per i sistemi che utilizzano ancora il boot loader LILO vedi 8.2 nella pagina seguente .

Exempio 8.2: *Il file /etc/lilo.conf*

```
boot    = /dev/hda
change-rules
reset
read-only
menu-scheme = Wg:kw:Wg:Wg
prompt
timeout = 80
message = /boot/message

  image  = /boot/vmlinuz
  label  = home
  root   = /dev/hda6
  initrd = /boot/initrd
  append = "vga=0x317 hde=ide-scsi PROFILE=home"

  image  = /boot/vmlinuz
  label  = work
  root   = /dev/hda6
  initrd = /boot/initrd
  append = "vga=0x317 hde=ide-scsi PROFILE=work"

  image  = /boot/vmlinuz
  label  = road
  root   = /dev/hda6
  initrd = /boot/initrd
  append = "vga=0x317 hde=ide-scsi PROFILE=road"
```

Ora al momento del boot potete scegliere comodamente il profilo che desiderate.

8.2.8 Difficoltà e la loro risoluzione

Di solito SCPM funziona senza causare delle difficoltà, ma a volte potrebbero verificarsi delle difficoltà che descriveremo di seguito.

Attualmente SCPM non è in grado di amministrare gli aggiornamenti di sistema, dato che i dati salvati nei profili non possono venir aggiornati dai diversi meccanismi di aggiornamento. SCPM riconosce se è stato effettuato un aggior- namento del sistema e rifiuterà in tal caso i propri servigi. In questi casi otterrete da SCPM un messaggio di errore del tipo "Installazione del sistema operativo modificata o non nota". In questi casi reinizializzate

SCPM con `scpm -f enbale`. I profili comunque andranno persi, e quindi vanno ricreati.

Eventualmente può verificarsi 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 e simili - oppure ad un errore in SCPM. In questo caso la prossima volta che invocate SCPM appare il messaggio di sistema che SCPM è bloccato. Ciò protegge 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 cancellate il file lock con `rm /var/lib/scpm/#LOCK` e ripristinate con `scpm -s reload` uno stato consistente; in seguito potete continuare a lavorare normalmente.

Ancora una indicazione: in linea di massima modificare la configurazione dei gruppi di risorsa con SCPM in esecuzione non crea delle difficoltà. Non dimenticate che dopo aver aggiunto o eliminato dei gruppi, va invocato `scpm rebuild` per aggiungere nuove risorse a tutti i profili e cancellare quelle eliminati. Quest'ultime saranno cancellate in modo definitivo; se li avete 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 un comando rebuild, YaST lo eseguirà automaticamente.

8.3 IrDA – Infrared Data Association

IrDA (ingl.*Infrared Data Association*) è uno standard industriale per la comunicazione wireless tramite 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 range tra i 2400 bps ed i 4 Mbps.

IrDA ha due modi di funzionamento. 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 per ogni di questi chip. Inoltre va impostato 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/

8.3.1 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.

8.3.2 Configurazione

Il sistema di servizio IrDA non viene avviato automaticamente al boot. Usate il modulo runlevel di YaST per modificare le impostazioni dei servizi di sistema. Un'altra possibilità consiste nell'usare il programma chkconfig. Purtroppo il consumo energetico di IrDA è decisamente superiore rispetto ad altri componenti, poichè ad intervalli brevissimi (pochissimi secondi) viene inviato un pacchetto cosiddetto discovery per il rilevamento automatico delle altre periferiche. Così si consiglia, soprattutto se è la batteria ad alimentare il sistema, di avviare IrDA solo nel caso di necessità; con il comando rcirda start attivate l'interfaccia manualmente e con il parametro stop la disabilitate. Quando attivate l'interfaccia, tutti i moduli del kernel necessari vengono caricati automaticamente.

Nel file /etc/sysconfig/irda c'è solo una variabile IRDA_PORT. Potete impostare quale interfaccia debba venire usata nella modalità SIR; ciò viene impostato tramite lo script /etc/irda/drivers durante l'attivazione del supporto per i raggi infrarossi.

8.3.3 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 un'interfaccia normale /dev/lp0, con la sola differenza che i dati da stampare vengono inviati wireless tramite i raggi ad infrarossi.

Una stampante che viene usata tramite una porta ad infrarossi, si lascia configurare come una stampante collegata alla porta parallela o seriale. Quando stampate dovete considerare che la stampante deve trovarsi nei pressi della porta ad infrarossi del computer e che sia attivato il supporto per la luce infrarossa.

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, grazie ai raggi infrarossi, senza aver bisogno dei cavi ovvero wireless ad Internet tramite il programma wvdial. Potete anche allineare i vostri dati con il Palm Pilot, basta immettere nel rispettivo programma `/dev/ircomm0` come dispositivo.

Tenete presente che potete indirizzare solo dispositivi che supportano i protocolli Printer o IrCOMM, leggete a riguardo l'IR-HOWTO. Con programmi particolari (irobexpalm3, irobexreceive, potete indirizzare anche dispositivi che utilizzano il protocollo IROBEX (3Com Palm Pilot). I protocolli supportati dal dispositivo vengono indicati nella parentesi quadra dopo i nomi dei dispositivi nell' output di irdadump. I supporto del protocollo IrLAN si trova in fase di sviluppo – purtroppo non funziona ancora in modo stabile, ma di sicuro in un futuro prossimo sarà disponibile anche per Linux.

8.3.4 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. output 8.3.

Exempio 8.3: *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 stato

usando un interrupt diverso da Interrupt 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 infrarossi – a differenza dell'occhio umano la maggior parte delle videocamere riesce a vedere i raggi infrarossi.

8.4 Bluetooth – connessione wireless

Bluetooth permette di far interagire tra loro diversi dispositivi senza la necessità di una connessione via cavo. Bluetooth si differenzia da IrDA in quanto i singoli dispositivi non devono "vedersi" direttamente e in quanto 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 1.1). 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.

8.4.1 I cosiddetti 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.

8.4.2 Software

Per poter utilizzare la tecnologia Bluetooth serve un adapter per Bluetooth (sia esso integrato nel dispositivo o un dongle esterno), 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. Inoltre vanno installati tutti i pacchetti riferiti a Bluetooth (`bluez-libs`, `bluez-bluefw`, `bluez-pan`, `bluez-sdp` e `bluez-utils`), dato che forniranno alcuni servizi e programmi di servizio richiesti; alcuni verranno illustrati di seguito.

8.4.3 La configurazione

I file descritti di seguito possono essere modificati solo da `root`. Attualmente purtroppo non vi è un'interfaccia grafica tramite la quale poter impostare i parametri, quindi bisogna ricorrere ad un editor di testo.

Per tutelarsi contro connessioni involontarie vi sono i codici PIN. I telefonini ad esempio richiedono il codice PIN al primo contatto o durante il processo di configurazione riguardante il contatto tra dispositivo e telefonino. Entrambi i dispositivi devono autenticarsi con lo stesso codice PIN per consentire la comunicazione. Il codice si trova nel file `/etc/bluetooth/pin`. Attualmente in Linux vi è un solo PIN, indipendentemente dal numero dei dispositivi Bluetooth installati. Purtroppo al momento non è possibile indirizzare diversi dispositivi con differenti PIN, in questi casi si dovrà impostare lo stesso codice PIN per tutti i dispositivi o si dovrà disabilitare il processo di autenticazione basato sul PIN.

Nota

Connessioni tramite Bluetooth e la sicurezza

Nonostante i codici PIN, bisogna tenere presente che è possibile intercettare la comunicazione tra due dispositivi!

Nota

L'abilitazione avviene tramite il file di configurazione `/etc/bluetooth/hcid.conf`. Qui potete modificare diverse impostazioni come ad esempio il nome di dispositivo e la modalità di sicurezza. In linea di massima queste impostazioni dovrebbero rilevarsi sufficienti, in questa sezione ne illustreremo brevemente due. Il file contiene dei commenti che descrivono le opzioni delle singole impostazioni.

Una della impostazioni più importanti è `security auto;` che abilita l'autenticazione in base al PIN, laddove in caso di difficoltà `auto` può essere impostato su `Non utilizzare PIN`. La decisione se impostare qui `none` in modo da non utilizzare mai un codice PIN oppure su `user` (utilizzarlo sempre), dipende dai vostri criteri di sicurezza.

Di sicuro interesse è la sezione che inizia con `device {`. Qui potete stabilire con quale nome debba essere visualizzato l'host sulle controparti. Qui definite la classe dei dispositivi (`Laptop`, `Server`, etc.) come anche l'autenticazione ed il metodo di cifratura.

8.4.4 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 e che permette di gestire il dispositivo Bluetooth) e sdpd (*Service Discovery Protocol* che comunica i servizi offerti dal client). 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 per poter utilizzare Bluetooth. Purtroppo al momento esistono solo dei programmi da riga di comando. Alla chiusura redazionale non era chiaro se la distribuzione presenterà una estensione per il browser di Konqueror (KDE-Desktop) o di Nautilus (GNOME-Desktop). In caso affermativo l' URL `sdp://` dovrebbe visualizzare dispositivi Bluetooth locali ovvero connessi al computer e dispositivi Bluetooth remoti ovvero indirizzabili solo via etere.

Nota

Tutti i programmi menzionati offrono anche ulteriori funzionalità; consultate a riguardo la pagina di manuale con `man <nomeprogramma>`.

Nota

Alcuni comandi possono essere eseguiti solo da `root`, come ad es. `l2ping <indirizzo_del_dispositivo>`, 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` sarà visualizzato il vostro dispositivo. L'output presenta una riga del tipo `<nome_dell'_interfaccia> <indirizzo_del_dispositivo >` per ogni dispositivo locale rilevato.

Con `hcitool nome <indirizzo_del_dispositivo>` potete rilevare il nome di dispositivo anche di un dispositivo remoto. Se si tratta ad es. di un ulteriore computer la classe ed il nome di dispositivo risultanti corrisponderanno a quanto specificato nel rispettivo file `/etc/bluetooth/hcid.conf`. Indirizzi di dispositivi locali ritornano un messaggio di errore.

hciconfig

`/sbin/hciconfig` fornisce ulteriori informazioni sul dispositivo locale. Per eseguire una ricerca dei dispositivi remoti, dunque non connessi al computer, si immette `hcitool inq`. Per ogni dispositivo rilevato verranno emessi tre valori: l'indirizzo del dispositivo, il clock offset e la classe del dispositivo. L'indirizzo del dispositivo viene utilizzato nei comandi per identificare il dispositivo meta. Il clock offset è di interesse solo da un punto di vista tecnico. Il tipo di dispositivo e di servizio viene codificato nella classe sotto forma di un valore esadecimale.

sdptool

sdptool vi informa sul servizio offerto da un determinato dispositivo. `sdptool browse <indirizzo_del_dispositivo>` ritorna tutti i servizi del dispositivo, mentre con `sdptool search <sigla._del_servizio>` si può cercare in modo mirato un determinato servizio. Con questo comando vengono interrogati tutti i dispositivi raggiungibili per quel che riguarda il servizio richiesto. Se un dispositivo mette a disposizione il servizio cercato, il programma ritorna il nome completo ed una breve descrizione del dispositivo. Eseguendo `sdptool` senza alcun parametro si ottiene un elenco delle sigle dei servizio.

8.4.5 Esempi

Per dare una dimostrazione delle capacità di Bluetooth, riportiamo di seguito due esempi.

Collegamento via rete tra due host H1 e H2

Nel primo esempio vogliamo creare un collegamento di rete tra due host, cosa resa possibile da pand (*Personal Area Networking*). I seguenti comandi devono essere eseguiti dall'utente `root`. Non ci soffermeremo sui dettagli per quel che riguarda i comandi di rete (ip), ci concetreremo invece sulle azioni che riguardano da vicino Bluetooth:

Su uno dei due host (di seguito *H1*) si lancia pand dando il comando `pand -s`. Il secondo host *H2* ne rivela indirizzo di dispositivo con `hcitool inq`. Con `pand -c <indirizzo_ del_dispositivo>` si può creare un collegamento. Invocando a questo punto l'elenco delle interfacce di rete disponibili tramite `ip link show` 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. Dopo aver assegnato a questa interfaccia un indirizzo IP bisogna attivarlo.

Per realizzare ciò, si immettono i seguenti due comandi su *H1*:

```
ip addr add 192.168.1.3/24 dev bnep0
ip link set bnep0 up
```

o per *H2* si ha:

```
ip addr add 192.168.1.4/24 dev bnep0
ip link set bnep0 up
```

Da considerare che il 3 diventa un 4. In tal maniera, *H1* può essere indirizzato da *H2* sotto l'indirizzo IP `192.168.1.3`. Con `ssh 192.168.1.4` potete collegarvi da *H1* a *H2* (se su *H2* gira un sshd, come di default per 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 apposito cellurare (senza creare costi aggiuntivi ad es.: dovuti all'invio di una mail multimediale) sul computer. Chiaramente il modo in cui sono strutturati i menu del cellulare varia da modello a modello, ma il modo di procedere non si discosta più di tanto. All'occorenza consultate la guida del vostro cellulare. La descrizione qui riportata si riferisce ad una foto scattata con un Sony Ericsson da trasferire sul portatile. Per realizzare questo trasferimento sul portatile è richiesto il servizio Obex-Push ed esservi consentito l'accesso anche al cellulare. Innanzitutto dobbiamo abilitare il servizio sul portatile, utilizzando il demone opd del pacchetto `bluez-utils`. Lanciatelo con:

```
opd --mode OBEX --channel 10 --daemonize --path /tmp --sdp
```

Due parametri sono di rilievo. `--sdp` comunica il servzio 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 avere l'accesso in scrittura per la directory indicata.

Ora "presentate" il portatile al celluare. 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 appartenente al portatile. A questo punto vi dovrebbe venir richiesto il codice PIN, immettete qui il codice PIN preso da `/etc/bluetooth/pin`. Ora il vostro cellulare conosce 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 potete tramite 'Invia' 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 pezzo musicale sul vostro portatile.

8.4.6 Come risolvere possibili difficoltà

Se dovessero verificarsi dei problemi di connessione procedete come descritto di seguito:

- Controllate l'output di `hcitool dev`. Viene visualizzato il dispositivo locale? In caso negativo ciò potrebbe essere dovuto al fatto che hcid non sia in esecuzione oppure al fatto che il dispositivo non venga riconosciuto come dispositivo Bluetooth (manca il driver oppure il dispositivo è rotto). Riavviate il demone con `rcbluetooth restart` e date una occhiata a `/var/log/messages` per vedere se si sono verificati degli errori.
- Il sistema "vede" gli altri dispositivi se immettete `hcitool inq`? Provatelo più volte, può darsi che la connessione non funzioni in modo ineccepibile. La banda di frequenze per Bluetooth viene utilizzata anche da altri dispositivi.
- Controllate, se il codice PIN in `/etc/bluetooth/pin` ed il PIN dell'altro dispositivo concordano.

- Provate a realizzare la connessione dall'altro dispositivo, verificate se il dispositivo vede il portatile.
- Se il primo esempio non porta all'effetto desiderato (Connessione via rete), la causa può essere dovuta a diverse ragioni: può darsi che uno dei computer non supporti il protocollo ssh. Eseguite un test con: `ping 192.168.1.3` o `ping 192.168.1.4`. Se funziona, controllate se é in esecuzione sshd. Una altra causa per l'insorgere di difficoltà può essere dovuta ad un conflitto di indirizzi (nell'esempio `192.168.1.X`). Provate con altri indirizzi, ad es. `10.123.1.2` e `10.123.1.3`.
- Nel secondo esempio il portatile non viene visualizzato come dispositivo meta: il telefonino riconosce 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 dovuto 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? La risposta è affermativa, alcuni dispositivi lo consentono (Siemens e Sony Ericsson sono stati testati, anche altri lo possono fare ma non è detto che lo facciano): installate obexftp ed eseguite `obexftp -b <indirizzo_del_dispositivo> -B 10 -p <foto>`.

8.4.7 Ulteriori informazioni

Per una valida rassegna delle diverse guide incentrate sull'utilizzo e la configurazione di Bluetooth, visitate il seguente sito: `http://www.holtmann.org/linux/bluetooth/`

Informazioni e guide:

- Connessione con PalmOS PDA (inglese): `http://www.cs.ucl.ac.uk/staff/s.zachariadis/btpalmlinux.html`

L'how-to ufficiale per il *Bluetooth Protocol Stack* integrato nel kernel: `http://bluez.sourceforge.net/howto/index.html`

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, cosa che aiuta a realizzare un risparmio energetico in particolar modo su dispositivi mobili alimentati dalla batteria (*CPU Frequency Scaling*).

Il power management presuppone hardware adatto e routine BIOS adatte. La maggior parte dei portatili e tanti desktop moderni hanno i presupposti per consentire il power management. Finora si è usato lo standard APM (*Advanced Power Management*). Si tratta di funzionalità implementate nel BIOS del computer. Per tale ragione il power management 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 sul vostro hardware e adottate la tecnologia che meglio si addice al vostro ambiente.

Nota

Power management su processori AMD64

I processori AMD64 supportano in combinazione con un kernel a 64 bit esclusivamente l' ACPI.

Nota

9.1 Funzionalità per il risparmio energetico

Queste funzioni sono di interesse generale, ma soprattutto in correlazione coi portatili. Descriveremo queste funzioni e spiegheremo quale sistema li supporta.

Stand-by In questo caso è solo lo schermo ad essere spento e ridotta l'attività del processore. Non tutti gli APM mettono a disposizione questa funzionalità. Corrisponde allo stato *S1* dell'*ACPI*.

Suspend (to memory) Il completo stato del sistema viene scritto nella RAM e viene sospeso il funzionamento del resto del sistema. Il computer consuma così poca energia ed, a seconda del 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 monitor per entrare nella modalità Suspend (to memory) e rialzarlo per continuare a lavorare. Corrisponde allo stato *S3* dell'*ACPI*.

Hibernation (Suspend to disk) Qui lo stato del sistema viene salvato sul disco fisso ed in seguito spento il sistema. Dura tra i 30 fino ai 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*.

Controllo dello stato della batteria
Oltre a controllare lo stato di caricamento della batteria, bisogna agire quando le riserve di energia stanno per esaurirsi. Questa funzione di controllo può essere svolta da ACPI o APMA.

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 ad avere 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 via ACPI almeno in teoria temporaneamente o permanentemente nel BIOS setup.

Controllo dell'attività del processore
PowerNow! di AMD e SpeedStep di Intel mirano a ridurre il consumo energetico del sistema nel suo intero ed in particolare della sua componente a maggior consumo energetico ovvero il processore. Un ulteriore effetto positivo dell'attività ridotta del processore è che si produce meno calore così che ventole a velocità regolabile possono lavorare meno rumorosamente. Le funzioni *CPU Frequency Scaling* del kernel Linux regolano questo processo. In questo contesto si distingue principalemente tra tre livelli dell'attività del processore:

performance massima performance del processore — indicato se il sistema è connesso alla rete elettrica esterna.

powersave attività minima del processore per il funzionamento a batteria

dynamic adattamento dinamico dell'attività del processore al carico di lavoro attuale — impostazione preferibile sia ad alimentazione esterna che a batteria volta a prolungare la durata della batteria, ridurre i rumori di sottofondo e realizzare un'ottima performance. In condizioni normali il passaggio da uno stadio all'altro avviene in modo impercettibile per l'utente.

Per maggiori informazioni su come regolare l'attività del processore rimandiamo alla sezione 9.5 a pagina 238.

9.2 APM

Alcune funzionalità di risparmio energetico vengono eseguite autonomamente dal BIOS APM. Spesso gli stati di stand-by e suspend si lasciano attivare con una combinazione di tasti o abbassando lo schermo. In questi casi non è necessaria alcuna funzionalità del sistema operativo. Chi però vuole che questi stati vengano indotti da un comando e che vengano eseguite delle particolari azioni o che venga semplicemente indicato lo stato di caricamento della batteria, deve aver installato 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 BIOS APM. Per attivare il supporto di APM, bisogna spegnere ACPI al prompt di boot con `acpi=off`. Potete controllare con il comando `cat /proc/apm` se l'APM è stato attivato. 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 parametri di boot particolari (prima erano delle opzioni di configurazione del kernel). Tutti i parametri vengono immessi al prompt di boot sotto forma di `apm=<parametro>`:

on/off Accendere/spegnere il supporto APM

(no-)allow-ints Permettere degli interrupt durante l'esecuzione delle funzioni del 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 (realmode).

(no-)debug Protocollare gli eventi APM nel syslog.

(no-)power-off Spegnere il sistema dopo lo shutdown.

bounce-interval=⟨*n*⟩ Tempo in centesimi di secondo, in cui vengono ignorati ulteriori suspend dopo un evento suspend.

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 tramite i quali determinare l'(in)attività del sistema.

9.2.1 Il demone APM (apmd)

Il demone `apmd` vigila sullo stato della batteria e può far scattare determinate azioni se si entra nella modalità stand-by o suspend. Lo trovate nel pacchetto `apmd`. Non è indispensabile per il funzionamento del sistema, ma può rilevarsi molto utile in alcuni casi per risolvere dei problemi.

L'`apmd` non viene inizializzato automaticamente al boot. Comunque le impostazioni riguardanti i servizi di sistema si lasciano modificare nel modulo dei runlevel di YaST, oppure potete usare il programma `chkconfig`. Con il comando `rcapmd start` potete inizializzarlo manualmente.

Ai fini della configurazione vi sono delle variabili in `/etc/sysconfig/powermanagement`; il file contiene dei commenti, così in questa sede ci limiteremo a dare solo delle indicazioni generali.

APMD_ADJUST_DISK_PERF Con questa variabile potete adeguare la performance del disco fisso allo stato della alimentazione energetica. Esistono a riguardo inoltre una serie di variabili che iniziano con `APMD_BATTERY` o `APMD_AC`. Le prime si riferiscono ad impostazioni relative all'alimentazione a batteria e le seconde all'alimentazione esterna.

APMD_BATTERY/AC_DISK_TIMEOUT
Indica dopo quando tempo di inattività del disco rigido esso viene fermato. I valori possibili vengono descritti nella sezione 9.4 a pagina 236 o nella pagina di manuale di `hdparm` opzione `-S`.

APMD_BATTERY/AC_KUPDATED_INTERVAL
Il tempo tra due esecuzioni del demone di aggiornamento del kernel (ingl. kernel update deamon).

APMD_BATTERY/AC_DATA_TIMEOUT
il tempo di permanenza massimo per i dati nel buffer.

APMD_BATTERY/AC_FILL_LEVEL
Il limite di riempimento massimo del buffer del disco fisso.

APMD_PCMCIA_EJECT_ON_SUSPEND
Nonostante PCMCIA sia compilata con supporto APM, a volte subentrano dei problemi. Alcuni driver di schede non si "risvegliano" correttamente dalla modalità suspend (`xirc2ps_cs`), per cui l'apmd può disattivare il sistema PCMCIA prima di entrare nella modalità suspend ed riattivarlo in seguito, impostando la variabile `APMD_PCMCIA_EJECT_ON_SUSPEND` su `yes`.

APMD_INTERFACES_TO_STOP Qui potete indicare le interfacce di rete che dovranno essere spente prima di entrare nella modalità suspend e da reinizializzare successivamente.

APMD_INTERFACES_TO_UNLOAD
Utilizzate questa variabile se vanno scaricati anche i moduli del driver di questa interfaccia.

APMD_TURN_OFF_IDEDMA_BEFORE_SUSPEND
A volte succede che non funzioni il "risveglio" dalla modalità di suspend se un dispositivo IDE (disco fisso) si trova ancora nel modo DMA.

Vi sono anche altri modi per correggere ad es. la velocità di ripetizione dei tasti o l'orario dopo la sospensione, o di eseguire automaticamente lo shutdown del portatile quando il BIOS AMP segnala "un evento critico" riguardante la batteria. Chi volesse eseguire prima delle azioni particolari ha la possibilità di adattare alle proprie esigenze lo script `/usr/sbin/apmd_proxy` che esegue gli incarichi descritti sopra.

9.2.2 Ulteriori comandi

apmd contiene ancora una serie di programmi utili. Con `apm` potete farvi indicare lo stato attuale della batteria e mandare il sistema nella modalità stand-by (`apm -S`) o suspend (`apm -s`); cfr. la pagina di manuale di `apm`. Il

comando `apmsleep` sospende il sistema per un lasso di tempo prestabilito. Chi vuole consultare un file di log senza mantenere continuamente attivo il disco rigido può usare `tailf` al posto di `tail -f`.

Chiaramente vi sono anche dei strumenti per il sistema X Window. apmd contiene anche xapm che mostra in modo grafico lo stato di caricamento della batteria. Chi usa il desktop KDE – o almeno kpanel –, può visualizzare lo stato di caricamento della batteria anche con kbatmon e sospendere ogni attività del sistema. Alternativamente è di sicuro interesse anche xosview.

9.3 ACPI

ACPI sta per *Advanced Configuration and Power Interface*. ACPI permette al sistema operativo di configurare e controllare singolarmente le componenti di 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 "Chiudere il coperchio" o "Batteria quasi scarica".

Il BIOS mette a disposizione delle tabelle in cui trovare 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. Lì ACPI indica quali tabelle ha rilevato e letto. Per maggiori informazioni su come risolvere dei problemi dovuti all'ACPI rimandiamo alla sezione 9.3.1 a pagina 235.

9.3.1 Nella prassi

Se all'avvio il kernel rivela un BIOS ACPI, 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` si può vedere se l'ACPI è stato attivato. Vi è anche la directory `/proc/acpi/` che viene descritta di seguito.

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 ineccebile 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 `echo X <file>` dei valori appropriati per X (`/proc` non contiene file, si tratta piuttosto di un' interfaccia per il kernel). 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 ibernazione.

`/proc/acpi/event` Qui vengono segnalati tutti gli eventi che vengono elaborati da un demone come `acpid` o `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 se si preme brevemente sul pulsante per l'accensione o se si abbassa il monitor.

`/proc/acpi/dsdt` e `/proc/acpi/fadt`
Qui trovate le tabelle ACPI: DSDT (*Differentiated System Description Table*) e *FADTemphasis>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: `acpidmp DSDT | acpidisasm`.

`/proc/acpi/ac_adapter/AC/state`
L'alimentatore è connesso?

`/proc/acpi/battery/BAT*/{alarm,info,state}`
Informazioni dettagliate sullo stato delle batterie. 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 di cui segue una descrizione. In `alarm` potete impostare un valore per innescare un evento di batteria.

/proc/acpi/button Qui trovate delle informazioni su vari bottoni.

/proc/acpi/fan/FAN/state Indica se la ventola è in funzione. Essa può venir accesa o spenta manualmente immettendo 0 (=on) o 3 (=off) in questo file. Comunque dovete considerare che sia il codice ACPI nel kernel che anche l'hardware (o il BIOS) possono sovrascrivere questa impostazione se vi è surriscaldamento.

/proc/acpi/processor/CPU0/info
Informazioni sulle possibilità di risparmio energetico per il processore.

/proc/acpi/processor/CPU*/power
Informazioni sullo stato attuale del processor. Un asterisco vicino a 'C2' sta per inattività; questo è lo stato più frequente, come mostra la cifra `usage`.

/proc/acpi/processor/CPU*/performance
Questa interfaccia non viene più utilizzata.

/proc/acpi/processor/CPU*/throttling
Qui è possibile un ulteriore throttling lineare del processore. Si tratta di un'interfaccia datata, che può dirsi sostituita dalle impostazioni che trovate sotto `/etc/sysconfig/powersave/common` (vedi la sezione 9.5.2 a pagina 241).

/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. Adesso questa funzione viene svolta dalle impostazioni sotto `/etc/sysconfig/powersave/common` (vedi la sezione 9.5.2 a pagina 240).

/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 denominazione vengono stati stabiliti dal 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 che 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 (ACPI) raffredda in modo "attivo" o "passivo". Tutto è "ok" se il controllo della ventola non dipende dall'ACPI.

/proc/acpi/thermal_zone/*/cooling_mode
Qui si può selezionare il metodo preferito di raffreddamento controllato pienamente 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").

/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 la l'indicazione della temperatura venga aggiornata ogni X secondi. Con X=0 si disabilita nuovamente il "polling".

Il demone ACPI (acpid)

Alla stregua del demone APM anche il demone ACPI elabora determinati eventi ACPI, per ora solo eventi che riguardano certi pulsanti come quello on/off oppure l'abbassare dello schermo. Tutti gli eventi vengono protocollati nel systemlog. In `/etc/sysconfig/powermanagement` potete stabilire con le variabili `ACPI_BUTTON_POWER` e `ACPI_BUTTON_LID` cosa debba succedere al verificarsi di questi eventi. Coloro che vogliono di più, possono modificare lo script `/usr/sbin/acpid_proxy` o la configurazione di `acpid` sotto `/etc/acpi/`.

Al contrario di `apmd`, qui non vi è tanto ad essere preconfigurato, visto che l'ACPI sotto Linux si trova in piena fase di sviluppo. All'occorrenza bisogna configurarsi l'`acpid` da soli. Se avete delle proposte da farci, potrete contattarci (preferibilmente in inglese)sotto `http://www.suse.de/feedback`.

Ulteriori tool

Vi sono 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`).

Possibili problemi e soluzioni

Potrebbero esserci degli errori passati inosservati nel codice ACPI del kernel, comunque in questi casi - non appena vengono scoperti - sarà messa a 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 riportata in cosiddette black list che a causa di gravi errori nella implementazione ACPI non possono essere utilizzate 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 configurazione delle risorse semplice.

acpi=off non utilizzare ACPI.

Attenzione

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 può comportare delle difficoltà.

Attenzione

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 almeno per la tabella più importante, la DSDT, integrare una tabella ottimizzata nel kernel. In tal modo viene ignorata la tabella DSDT del BIOS che contiene degli errori. La procedura da seguire viene illustrata nella sezione 9.5.4 a pagina 242.

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. Non nuoce neanche comunicare al vostro produttore di hardware che utilizzate Linux, anche se tutto funziona correttamente.

Per ulteriore documentazione ed assistenza consultate le seguenti fonti:

- `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)

9.4 Un breve intervallo per il disco rigido

Linux vi permette di spegnere il disco rigido quando non vi serve attraverso il programma hdparm con il quale potete eseguire varie impostazioni che verranno applicate al disco rigido. Con l'opzione `-y` il disco rigido viene mandato 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 per 30 minuti.

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 dal volume della 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. Chi è in possesso di un sistema stabile può modificare queste impostazioni, però deve tenere conto che ne va della sicurezza dei dati.

Attenzione

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. In caso di incertezza non è consigliabile apportare delle modifiche.

Attenzione

Le impostazioni per il timeout del disco rigido, l'intervallo di kupdated, il livello che deve essere raggiunto prima che il buffer venga svuotato e la permanenza dei file possono essere salvati in duplice copia sotto `/etc/sysconfig/powermanagement`: una volta per il funzionamento a batteria e una volta per il funzionamento ad alimentazione esterna. Le variabili sono descritte nella sezione dedicata ad apmd 9.2.1 a pagina 229 e nel file stesso. Inoltre trovate delle informazioni riferiti a questo tema sotto `/usr/share/doc/packages/powerstate`.

Oltre a quanto descritto fin qui, anche i cosiddetti "Journaling File system" p.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 come si comportano i programmi che sta-

te 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 diventa trascurabile se l'intervallo per kupdated è stato esteso.

9.5 Il pacchetto powersave

Il pacchetto `powersave` è stato pensato appositamente per le 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 normali postazioni di lavoro e server (ad es:suspend/standby, funzionalità bottono 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 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 di hardware summenzionati (APM e ACPI si escludono a vicenda), vale la pena utilizzare il demone di powersave per regolare il risparmio eneregetico. Eventuali modifiche della configurazione dell'hardware vengono rilevate automaticamente dal demone.

Nota

Su powersave

Oltre al presente capitolo sono reperibili ulteriori informazioni sul pacchetto powersave anche sotto `/usr/share/doc/packages/powersave/README_POWERSAVE`.

Nota

9.5.1 Configurazione del pacchetto powersave

powersave si configura tramite diversi file:

/etc/powersave.conf Questo file serve al demone di powersave per delegare l'elaborazione degli eventi del sistema (*event*) al powersave_proxy. Questo file contiene già dei valori di default sensati che in linea di massima non è necessario modificare.

/etc/sysconfig/powersave/common
Questo file contiene la configurazione generale dello script di inizializzazione (`rcpowersave`) del proxy. Solitamente i valori di default possono essere assunti senza che vi sia la necessità di apportarvi delle modifiche.

/etc/sysconfig/powersave Questo file contiene variabili di configurazione per il demone di powersave.

/etc/sysconfig/powersave/scheme_*
Si tratta dei diversi schemi o detti anche profili che regolano il consumo energetico in base a dei determinati scenari di applicazione. Alcuni sono già preconfigurati e possono essere subito utilizzati senza che vi sia la necessità di apportare delle modifiche. Comunque sussiste inoltre la possibilità di archiviarvi anche propri profili.

9.5.2 Configurazione di APM ed ACPI

Suspend e Standby

Nel file `/etc/sysconfig/powersave/common` stabilite quali moduli o servizi vitali scaricare o fermare prima di un evento di suspend o standby. Quando si riaccenderà il sistema questi moduli e servizi verranno nuovamente caricati o avviati. I valori di default riguardano soprattutto moduli USB e moduli PCMCIA.

POWERSAVE_SUSPEND_RESTART_SERVICES=""
Indicate qui i servizi da riavviare dopo un evento suspend.

POWERSAVE_STANDBY_RESTART_SERVICES=""
Indicate qui i servizi da riavviare dopo un evento standby.

POWERSAVE_UNLOAD_MODULES_BEFORE_SUSPEND=""
Indicate qui i moduli da scaricare prima di un evento suspend.

POWERSAVE_UNLOAD_MODULES_BEFORE_STANBY=""
Indicate qui i moduli da scaricare prima di un evento standby.

Inoltre si dovrà assicurare che siano settate le seguenti opzioni standard per la corretta interpretazione di eventi suspend/standby, occurence/resume (cosa che si ha di solito ad installazione avvenuta di SUSE LINUX):

```
POWERSAVE_EVENT_GLOBAL_SUSPEND="prepare_suspend"
POWERSAVE_EVENT_GLOBAL_STANDBY="prepare_standby"
POWERSAVE_EVENT_GLOBAL_RESUME_SUSPEND="restore_after_suspend"
POWERSAVE_EVENT_GLOBAL_RESUME_STANDBY="restore_after_standby"
```

Nel file di configurazione del demone di powersave sotto `/etc/powersave.conf` questi eventi vengono correlati allo script `powersave_proxy` che viene eseguito appena si hanno i seguenti eventi (default ad installazione avvenuta):

```
global.suspend=/usr/sbin/powersave_proxy
global.standby=/usr/sbin/powersave_proxy
global.resume.suspend=/usr/sbin/powersave_proxy
global.resume.standby=/usr/sbin/powersave_proxy
```

Stati della batteria definiti dall'utente

Nel file `/etc/sysconfig/powersave` potete stabilire tre stati di caricamento della batteria (espressi in punti percentuali) raggiunti i quali il sistema emette degli avvertimenti e esegue determinati azioni.

```
POWERSAVED_BATTERY_WARNING=20
POWERSAVED_BATTERY_LOW=10
POWERSAVED_BATTERY_CRITICAL=5
```

Le azioni/script che verranno eseguiti non appena si scende sotto la soglia dei valori impostati vengono impostate nel file di configurazione del demone powersave (`/etc/powersave.conf`). Il tipo delle azioni viene configurato in `/etc/sysconfig/powersave/common`:

```
POWERSAVE_EVENT_BATTERY_NORMAL="ignore"
POWERSAVE_EVENT_BATTERY_WARNING="notify"
POWERSAVE_EVENT_BATTERY_LOW="notify"
POWERSAVE_EVENT_BATTERY_CRITICAL="suspend"
```

Le ulteriori opzioni sono riportate nel file di configurazione.

Adattare il consumo energetico alle diversi condizioni di lavoro

Potete correlare il comportamento del sistema al tipo dell'alimentazione energitica. 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/powersave.conf` l'esecuzione di determinate azioni viene delegata a `powersave_proxy` quando il sistema viene connesso o disconnesso alla o dalla rete elettrica. In `/etc/sysconfig/powersave/common` selezionate i scenari (detti "Schemes" o "Profile"):

```
POWERSAVE_AC_SCHEME="performance"
POWERSAVE_BATTERY_SCHEME="powersave"
```

Gli "Schemes" vengono archiviati nei rispettivi file sotto `/etc/sysconfig/powersave/`. Il loro nome si compone di: `nome_scheme dello schema`. Nell'esempio ne vediamo due: `scheme_performance` e `scheme_powersave`. Preconfiguratí sono `performance`, `powersave` e `acoustic` vengono forniti da SUSE. Tramite il modulo YaST per il power management potete elaborare in qualsiasi momento schemi esisteni crearni di nuovi, cancellare quelli esistenti o modificare la correlazione allo stato di alimentazione energetica del sistema.

9.5.3 Ulteriori feature ACPI

Se utilizzate ACPI potete determinare la reazione del vostro sistema tramite i cosiddetti "tasti ACPI" (Power, Sleep e "Schermo alzato", "Schermo abbassato"). In `/etc/powersave.conf` l'esecuzione delle rispettive azioni viene delegata a powersave_proxy. L'azione in sé viene stabilita nel file `/etc/sysconfig/powersave/common`. Per maggiori dettagli consulate il 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"
Se premete il tasto Sleep il sistema entra nel modo suspend.

POWERSAVE_EVENT_BUTTON_LID_OPEN="ignore"
Se alzate lo schermo non succede niente.

POWERSAVE_EVENT_BUTTON_LID_CLOSED="screen_saver"
Se abbassate lo schermo 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 ridurre il livello di attività della CPU.

9.5.4 Troubleshooting

Ecco le FAQ in tema di powersave.

- **Non riesco a circoscrivere il problema...**

  Date una occhiata a `/var/log/messages` dove vengono protocolli i messaggi di errore e di allerta. Se scorrendo il file non si individua 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 ora possibile circoscrivere il problema.

- **Dopo aver abilitato ACPI gli stati di batteria ed i tasti non reagiscono nel modo in cui sono stati configurati...**

  In caso di difficoltà dovute ad ACPI, con `dmesg|grep -i acpi` potete individuare nell'output di `dmesg` i messaggi che si riferiscono ad ACPI.

  A volte è necessario eseguire un aggiornamento del BIOS per risolvere la causa del problema. Visitate dunque il sito del produttore del portatile, e 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, cercate un DSDT aggiornata per il vostro sistema da sostituire alla vecchia tabella DSDT contenente degli errori del vostro BIOS, i seguenti siti potranno esservi di aiuto:

1. Scaricate il DSDT adatto 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 continuate con il 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 disintallate il kernel e utilizzate `mkinitrd` per creare un initrd verrà integrato il DSDT adatto e caricato al boot.

- **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 la CPU frequency. I dettagli sono reperibili sotto `/usr/src/linux/Documentation/cpu-freq/*`. Se è richiesto un determinato modulo o una determinata opzione, configurate ciò nel file `/etc/sysconfig/powersave/common` tramite le variabili `CPUFREQD_MODULE` e `CPUFREQD_MODULE_OPTS`.

- **Suspend/Standby non funziona. . .**

  Ecco le possibili cause da ricondursi al kernel che ostacolano su sistemi **ACPI** il modo suspend/standby:

  - Sistemi con oltre 1 GB di RAM al momento non supportano (ancora) il modo suspend
  - Sistemi multi-processori o sistemi con un processore P4 (con hyper threading) attualmente non supportono il modo suspend.

  L'errore può essere anche dovuto ad una implementazione errata del vostro DSDT (BIOS). In questo caso installare un nuovo DSDT come descritto in *Dopo aver abilitato ACPI gli stati di batteria ed i tasti non reagiscono nel modo in cui sono stati configurati . . . .*

Su sistemi **ACPI** e **APM**:

Non appena il sistema tenta di scaricare un modulo corroto, il proxy si blocca ed l'evento suspend non viene innescato. 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 intervendo sulle impostazioni in `/etc/sysconfig/powersave/common`:

```
POWERSAVE_UNLOAD_MODULES_BEFORE_SUSPEND=""
POWERSAVE_UNLOAD_MODULES_BEFORE_STANDBY=""
POWERSAVE_SUSPEND_RESTART_SERVICES=""
POWERSAVE_STANDBY_RESTART_SERVICES=""
```

- **Utilizzando ACPI: il demone di powersave non rivela quando viene raggiunto un certo livello di carica della batteria... ;**

  In ACPI, il sistema operativo può richiedere dal BIOS una comunicazione quando si scende sotto un certo livello di carica della batteria. Il vantaggio di questo metodo consiste di non dovere costantemente leggere lo stato della batteria cosa che frenerebbe le prestazioni del sistema. Comunque può darsi il caso che l'avvertimento secondo quanto emesso dal BIOS funzioni, ma che 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` su `yes` per forzare la lettura dello stato della batteria.

9.6 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 centro di controllo di YaST ('Sistema' → 'Power management') appare la prima maschera del modulo (si veda la sezione 9.1 nella pagina successiva), in cui selezionare gli

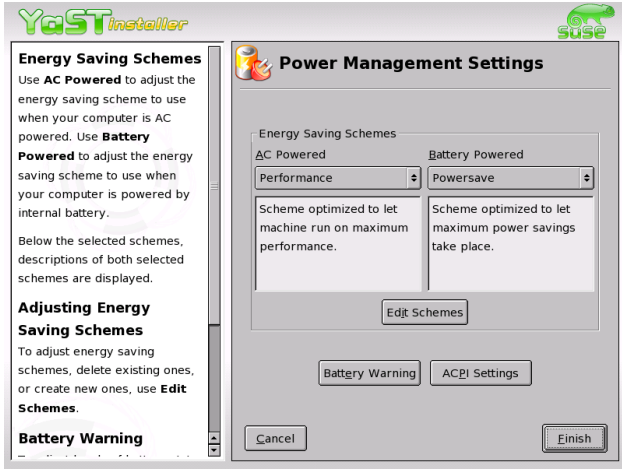

Figura 9.1: *YaST- power management: selezionare gli schemi*

schemi da utilizzare in base al modo di funzionamento — alimentazione a batteria o connessione alla rete elettrica —.

Avete la possibilità di selezionare uno schema esistente tramite il menu a tendina oppure visualizzare una panoramica degli schemi esistenti tramite il bottone 'Modifica schemi' (Fig. 9.2 nella pagina seguente).

Nella rassegna degli schemi selezionate lo schema che intendete modificare e cliccate su 'Modifica' per giungere al relativo dialogo (vedi 9.3 a pagina 247). Alternativamente potete crearne uno nuovo cliccando su 'Aggiungi'. In entrambi i casi segue lo stesso dialogo.

Date allo schema nuovo o da modificare innanzitutto un nome (qualificante) ed una descrizione. Stabilite una 'Standby Policy' volta a realizzare il massimo in termini di prestazioni o volta al risparmio energetico. L' 'Acoustic Policy' regola il livello di rumore del disco rigido. Cliccate su 'Prossimo' per giungere al dialogo sulla configurazione delle opzioni 'CPU' e 'Cooling Policy'. La voce 'CPU' include le opzioni 'CPU Frequency Scaling' e 'Throttling' che permettono di regolare la frequenza della CPU. La 'Cooling Policy' riguarda il tipo di raffredamento da applicare. Una volta che avete portato a termine l'impostazione dello schema uscite dal dialogo con 'OK' e ritornerete al dialogo iniziale (Fig. 9.1), dove potete attivare il vostro schema per uno dei due modi di funzionamento. Con 'OK' uscite dal dialogo e le vostre impostazioni diventano attive.

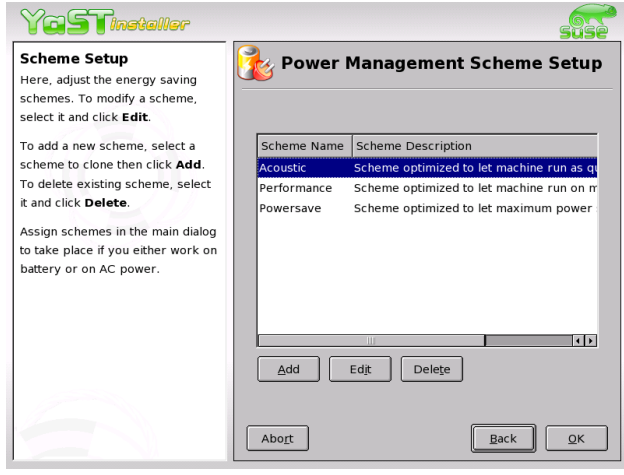

Figura 9.2: *YaST-power management: rassegna degli schemi esistenti*

Nel dialogo iniziale (si veda la figura 9.1 nella pagina precedente), potete eseguire anche impostazioni globali relative al power management accanto alla selezione dello schema per i diversi modi di funzionamento. Cliccate su 'Battery Warnings' o 'ACPI Settings'. Per giungere al dialogo sullo stato di caricamento della batteria, cliccate su 'Battery Warnings' (9.4 a pagina 248).

Non appena si scende sotto certi valori configurabili, il BIOS lo comunica al vostro sistema operativo e potrete determinare quale tipo di reazione dovrà seguire in risposta. In questo dialogo stabilite i tre valori di limite inferiore che una volta raggiunti o superati fanno scattare determinate azioni. Essi sono 'Warning Capacity', 'Low Capacity' e 'Critical Capacity'. Nei primi due casi, il messaggio di allerta raggiunge direttamente all'utente, mentre se si scende sotto l'ultimo livello critico il sistema entra nel modo di sospensione (suspend), 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; da lì giungete al dialogo di configurazione dei pulsanti ACPI tramite 'ACPI Settings' (si veda la fig. 9.5 a pagina 248).

Impostando i pulsanti ACPI stabilite il modo in cui debba reagire il sistema se si utilizzano determinati pulsanti. Questi pulsanti/eventi in ACPI si

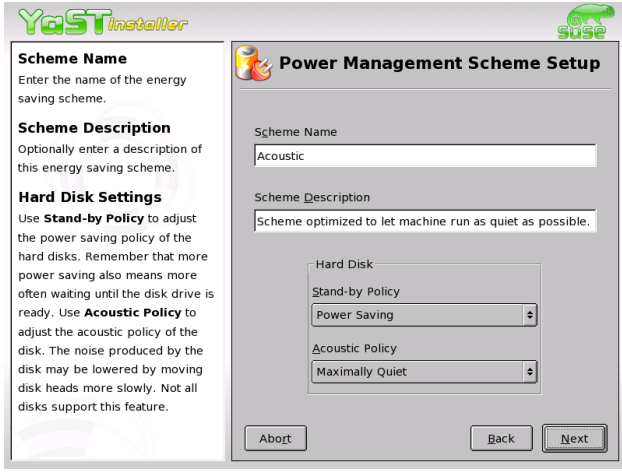

Figura 9.3: *YaST-power management: creare degli schemi*

chiamano “Buttons”. Configurate il tipo di risposta del sistema al premere del tasto (Power), del tasto (Sleep) ed all’abbassare dello schermo del portatile. Con ‘OK’ terminate la configurazione e ritornate al dialogo iniziale (Fig. 9.1 a pagina 245). Uscite dal modulo premendo nuovamente su ‘OK’ per rendere effettive le vostre impostazioni in tema di power management.

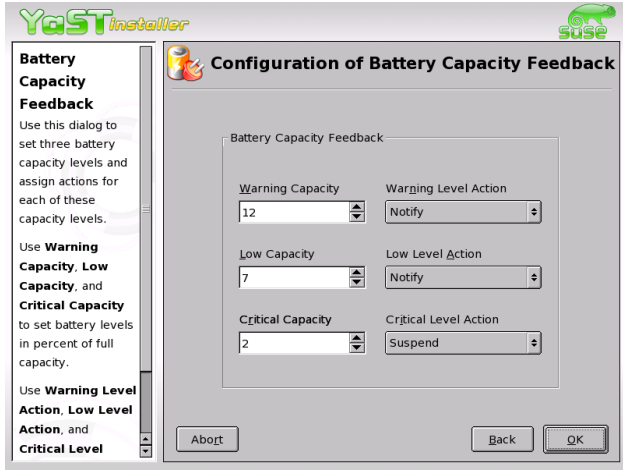

Figura 9.4: *YaST-power management: stato di caricamento della batteria*

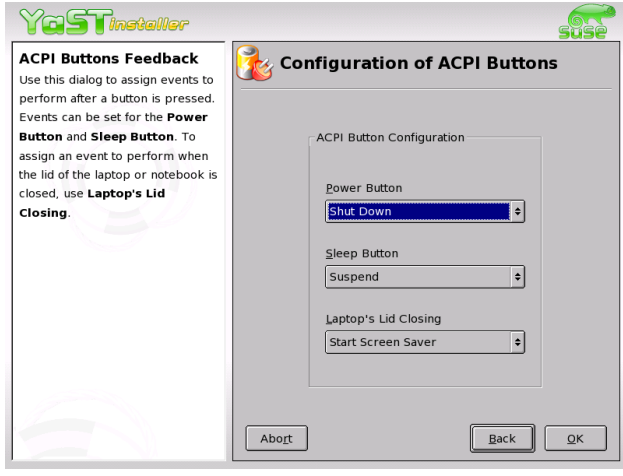

Figura 9.5: *YaST-power management: impostare l'ACPI*

Parte III

Sistema

SUSE LINUX su sistemi AMD64

Nel settembre del 2003 AMD ha presentato al pubblico il processore AMD Athlon64. Questo nuovo processore a 64 bit è quindi in grado di eseguire i nuovi programmi AMD64 a 64 bit. Inoltre è possibile continuare ad utilizzare i programmi x86 a 32 bit senza subire un calo di prestazioni.

I programmi a 64 bit offrono un maggior spazio di indirizzamento, e grazie a dei registri particolari supportati solo nel modo a 64 bit, nonché ad altre modifiche, come ad esempio per quel che riguarda le convenzioni di chiamata ("calling conventions") delle funzioni, si realizza una maggiore performance.

SUSE LINUX supporta il nuovo processore in due modi:

- Le versioni di SUSE LINUX a 32 bit per x86 supportano questo processore come processore a 32 bit così come supportano anche Athlon di AMD e il processore Pentium di Intel.
- Il nuovo SuSE Linux a 64 bit per AMD64 supporta il processore nel modo a 64 bit. Inoltre vengono supportati sia l'esecuzione che lo sviluppo di programmi x86 a 32 bit.

Nota

Per ragioni storiche l'output di `uname -m` è **x86_64**, visto che si tratta del nome della prima specifica di AMD.

Nota

10.1 SUSE LINUX a 64 bit per AMD64

10.1.1 Hardware

Sul lato hardware AMD64 non si distingue dagli altri sistemi Athlon AMD. Le comuni interfacce e bus sono identici su entrambe le piattaforme e vengono supportate.

Per quel che riguarda i driver hardware in parte dovranno essere apportati degli adattamenti. Alcune schede più datate al momento non funzionano, ma il supporto di hardware recente dovrebbe essere dato a 32 bit ed a 64 bit.

10.1.2 Software

Sul lato software abbiamo pacchetti a 64 bit. Si può comunque continuare ad utilizzare i programmi a 32 bit. Sono stati sviluppati appositamente dei pacchetti libreria a 32 bit che vengono installati durante l'installazione di

default. Per poter installare librerie a 32 bit ed a 64 bit omonimi su di un sistema, le librerie a 32 bit vengono installate nella directory `/lib/` e le librerie a 64 bit nella directory `/lib64/` che consente di installare RPM a 32 bit senza dover apportare delle modifiche.

Sul lato dell'amministrazione e delle applicazioni la differenza tra 32 bit e 64 bit non viene percepita direttamente, tutti i programmi hanno lo stesso aspetto e reagiscono nello stesso modo.

10.1.3 Installazione di software a 32 bit

Software a 32 bit che ricorre ad `uname` per rilevare l'architettura eventualmente va 'convinto' di girare su un sistema AMD64. Potrete utilizzare a tal fine il programma `linux32`, in seguito cambia l'output di `uname -m`:

```
$> uname -m

x86_64

$> linux32 uname -m

i686
```

10.1.4 Sviluppo software sotto i 64 bit

Su SUSE LINUX per sistemi AMD64 è possibile sviluppare sia programmi a 32 bit che a 64 bit. Il compiler GNU di solito generano un codice AMD64 a 64 bit. Con `-m32` si ha la generazione di codice x86 a 32 bit per sistemi Athlon a 32 bit di AMD oppure Pentium di Intel.

Quando si sviluppa codice a 64 bit bisogna utilizzare librerie a 64 bit. I percorsi `/lib64/` e `/usr/lib64/` saranno inclusi sempre nella ricerca, ma per codice X11 per esempio deve venir utilizzato `-L/usr/X11R6/lib64`. Quindi dovrete apportare degli adattamenti ai makefile.

Per il debug del codice si può utilizzare GDB, per programmi AMD64 a 64 bit vi è gdb, mentre per programmi x86 a 32 bit vi è gdb32. Il tool strace può analizzare sia programmi a 32 bit che a 64 bit e per il library tracer ltrace vi anche un programma a 32 bit:ltrace32.

10.2 Ulteriori informazioni

Per ulteriori informazioni rimandiamo al sito web di AMD (`www.amd.com`) e alla pagina dei progetti riguardanti il porting di Linux su AMD64 (`http://www.x86-64.org`).

Il kernel Linux

Il kernel è il cuore di un sistema Linux. Nelle prossime pagine, 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 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".

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.

11.1 Aggiornamento del kernel

Per installare un kernel di aggiornamento SuSE, scaricate il pacchetto di aggiornamento dal server ftp di SuSE o da un mirror come per esempio: `ftp://ftp.gwdg.de/pub/linux/suse/`. Se non sapete quale Kernel viene utilizzato attualmente sul vostro sistema, potete farvi mostrare la stringa indicante la versione `cat /proc/version`.

Inoltre potete verificare il pacchetto di cui fa parte il kernel `/boot/vmlinuz`:`rpm -qf /boot/vmlinuz`.

Prima della installazione, fate un back-up del kernel originale e del relativo `initrd`, immettendo come `root` i seguenti comandi:

```
cp /boot/vmlinuz /boot/vmlinuz.old
cp /boot/initrd /boot/initrd.old
```

Installate ora il nuovo pacchetto con: `rpm -Uvh <nomepacchetto>`. Inserite il corrispondente numero di versione.

A partire da SUSE LINUX 7.3 viene utilizzato reiserfs quale file system di default che presuppone l'uso di una "initial ramdisk" che viene riscritta con il comando `mk_initrd`. Nelle versioni recenti di SUSE LINUX ciò avviene automaticamente all'installazione del kernel.

Per poter avviare il vecchio kernel, si deve configurare il boot loader di conseguenza. I dettagli sono reperibili nel capitolo 7 a pagina 177.

Per installare il kernel originale di SUSE che trovate sui CD, dovete procedere in modo analogo. Sul CD 1 o DVD trovate nella directory `boot/` il kernel standard sotto forma di pacchetto rpm. Installatelo come descritto sopra. Se appare un messaggio di errore che vi comunica che è stato già

installato un pacchetto più recente, aggiungete al comando rpm l'opzione `--force`.

11.2 Le sorgenti del kernel

Per poter compilare un kernel è naturalmente necessario che siano installati i sorgente 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 installati automaticamente.

I sorgenti del kernel si trovano 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 in un dato 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.

11.3 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 nei 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.

11.3.1 Configurazione dalla riga 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 viene 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 (Enter) 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

11.3.2 Configurazione nel modo di testo

Per una configurazione più comoda, usate "menuconfig"; eventualmente dovete installare `ncurses-devel` con YaST. Iniziate 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.

11.3.3 Configurazione sotto il sistema X Window

Se avete installato il sistema X Window (il pacchetto `xf86`) e Tcl/Tk (il pacchetto `tcl` e il pacchetto `tk`), potete, in alternativa, eseguire la configurazione con `make xconfig`.

L'interfaccia grafica rende la configurazione più comoda. Il sistema X Window va inizializzato come utente `root` oppure immettete nella Shell come utente normale `xhost +` per concedere a `root` l'accesso al display. I valori di default vengono letti dal file `.config`. Tenete presente che la configurazione tramite `make oldconfig` non è così ben manutenuta come le altre possibilità di configurazione, quindi dopo questo metodo di configurazione eseguite un `make xconfig` .

11.4 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 cose simili vanno compilate direttamente nel kernel, mentre il supporto per `isofs`, `msdos` o `sound` dovrebbe essere compilato sotto forma di modulo.

I moduli del kernel vengono archiviati nella directory `/lib/modules/<versione>/`; dove `versione` corrisponde alla versione attuale del kernel.

11.4.1 Rilevamento dell'hardware attuale con hwinfo

SUSE LINUX vi offre il programma hwinfo per rilevare l'hardware del sistema e assegnare i driver disponibili. 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.

11.4.2 Utilizzo dei moduli

Per l'utilizzo dei moduli si hanno 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` .

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 degli altri moduli. Questo comando è molto utile e può venire impiegato anche per altri scopi (p.es. test di 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/conf.modules` 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 quali moduli che sono attualmente caricati vengono utilizzati da altri moduli. I moduli caricati dal demone del kernel sono contrassegnati con `(autoclean)`; ciò significa che questi moduli vengono automaticamente rimossi se non vengono usati per un certo periodo di tempo . Vedi però 11.4.4 a fronte.

modinfo Vi mostra i dettagli di un modulo.

11.4.3 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 CD-ROM o 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/`.

11.4.4 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 chiamate di 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. Per server che devono eseguire solo compiti speciali e che necessitano solo pochi driver si consiglia, per ragioni di prestazione, un kernel "monolitico".

11.5 Impostazioni della configurazione del kernel

Non è possibile descrivere in modo dettagliato le singole configurazioni possibili del kernel in questa sede: utilizzate i numerosi testi di aiuto riguardanti la configurazione del kernel. L'ultima versione della documentazione si trova sempre nella directory `/usr/src/linux/Documentation/`, se avete installato il pacchetto `kernel-source`.

11.6 Compilare il kernel

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 riga 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 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`.

11.7 Installare il kernel

Dopo aver compilato il kernel, dovete installarlo in modo da potere caricarlo d'ora in poi.

Se usate LILO, reinstallatelo. Nel caso più semplice, copiate il nuovo kernel sotto `/boot/vmlinuz` e lanciate poi LILO; per evitare brutte sorprese, è consigliabile in un primo momento avere a portata di mano il vecchio kernel (come `/boot/vmlinuz.old`), per poter eseguire il boot, nel caso il nuovo kernel non funzionasse a dovere.

```
cp /boot/vmlinuz /boot/vmlinuz.old
cp arch/i386/boot/bzImage /boot/vmlinuz
lilo
```

Il make file target `make bzlilo` esegue questi 3 passi in una sola volta.

Nota

Se come boot loader utilizzate GRUB, esso *non* deve essere reinstallato! Eseguite dunque solo i primi due passi per copiare il kernel nella parte del sistema giusta.

Nota

I moduli compilati devono ora solo essere installati; con il comando `make modules_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 originali ed il kernel.

Nota

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.

Nota

Affinché GRUB o LILO siano in grado di caricare il vecchio kernel (adesso `/boot/vmlinuz.old`) inserite nel file `/etc/lilo.conf` o `/boot/grub/menu.lst` inoltre l'etichetta `Linux.old` come immagine di boot. Questo procedimento viene spiegato dettagliatamente nel capitolo 7 a pagina 177. Se utilizzate LILO come bootloader, bisogna riavviarlo dopo aver modificato `/etc/lilo.conf`; cosa invece non necessaria con GRUB.

Da tenere 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 attuale `/usr/src/linux/System.map` nella directory `/boot/`. Questo file viene ricreato ad ogni compilazione del kernel. Se create il vostro kernel tramite `make bzlilo` oppure `make zlilo`, questo processo viene eseguito automaticamente.

Se al momento del 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/`.

11.8 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:

```
cd /usr/src/linux
make clean
```

Se, però, avete spazio a sufficienza sul disco e avete intenzione di riconfigurare spesso il kernel, saltate quest'ultimo punto. Quando ricompilerete il kernel, durerà meno, poiché vengono ricompilate solo quelle parti del sistema soggette a modifiche.

Caratteristiche del sistema

Questo capitolo contiene alcune informazioni sul *Filesystem Hierarchy Standard* (FHS) ed il *Linux Standard Base* (LSB), nonché su singoli pacchetti di software e particolarità del processo di caricamento con `initrd`, il programma linuxrc ed il Sistema di salvataggio.

12.1 Gli standard Linux

12.1.1 Linux Standard Base (LSB)

SUSE supporta attivamente gli sforzi del progetto *Linux Standard Base*; per informazioni aggiornate, visitate il sito `http://www.linuxbase.org`.

La specificazione LSB è arrivata alla versione 1.3.x. Ora il Filesystem Hierarchy Standard (FHS) è parte della specificazione e tra l'altro è stabilito il formato di pacchetto e l'inizializzazione del sistema; cfr. il capitolo 13 a pagina 293.

12.1.2 Filesystem Hierarchy Standard (FHS)

SUSE LINUX cerca di conformarsi al *Filesystem Hierarchy Standard* (FHS, il `fhs`); cfr.`http://www.pathname.com/fhs/`. Per questo motivo, di tanto in tanto, è necessario spostare file o indirizzari nei settori giusti del file system.

L'obbiettivo dell'FHS è di avere una struttura che ad esempio permette di montare `/usr` in sola lettura ovvero read-only.

12.1.3 teTeX – TeX su SuSE Linux

TeX è un complesso programma che gira su numerose piattaforme. E' estendibile tramite macro-pacchetti come LaTeX;. E' composto da numerosi file, da impostare secondo la *TeX Directory Structure* (TDS) (cfr. `ftp://ftp.dante.de/tex-archive/tds/`; teTeX è una raccolta di software TeX aggiornato.

Su SUSE LINUX, teTeX viene usato nel caso di una configurazione che debba soddisfare i requisiti sia della TDS che dell'FHS.

12.1.4 FTP

Per facilitare l'allestimento di un server FTP, il pacchetto `ftpdir` offre un esempio di ambiente, da installare sotto `/srv/ftp`.

12.1.5 HTTP

Apache è il server web standard di SUSE LINUX. Installando Apache avrete a disposizione dei documenti-esempio sotto `/srv/www`. Se volete allestire un proprio server web, registrate una propria `DocumentRoot` in `/etc/httpd/httpd.conf` e archiviate lì i vostri file (documenti, immagini etc.).

12.2 Informazioni su particolari pacchetti di software

12.2.1 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 dell'utente. Dopo un update si consiglia di orientarsi alle impostazioni di `/etc/skel`; per non perdere propri adattamenti eseguite questo comando:

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

In seguito dovete riscrivere i vostri adattamenti dal file `*.old`.

12.2.2 Il pacchetto cron

Le tabelle `cron` si trovano sotto `/var/cron/tabs`. Come tabella valida per tutto il sistema, viene creato il file `/etc/crontab`. Nel file `/etc/crontab`, dopo l'inserimento dell'ora, indicate anche sotto quale utente debba venire eseguito il relativo incarico (cfr. file 12.1, che indica `root`); i dati dei pacchetti in `/etc/cron.d` hanno lo stesso formato – cfr. la pagina di manuale `man cron`.

Exempio 12.1: *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, e 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 svolgono il compito della manutenzione quotidiana (il pacchetto `aaa_base`). In `/etc/cron.daily/` oltre a `aaa_base` vi è p.es. `backup-rpmdb`, `clean-tmp` o `clean-vi`.

12.2.3 File di log – il pacchetto logrotate

Molti servizi di sistema (*daemon*) ed il kernel stesso protocollano regolarmente lo stato del sistema od eventi particolari nei cosiddetti file protocollo (*logfiles*) 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.

Il passaggio a logrotate (8.0)

Nell'update di una versione antecedente a SUSE LINUX 8.0 vengono riprese le impostazioni precedenti:

- Tutti i file di `/etc/logfile` che non appartengano a determinati pacchetti, vengono spostati su `/etc/logrotate.d/aaa_base`.
- L'ex variabile `rc.config` `MAX_DAYS_FOR_LOG_FILES` viene riprodotta come `dateext` e `maxage` nel file di configurazione; cfr. `man logrotate`.

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 SUSE LINUX è previsto che i singoli pacchetti di `/etc/logrotate.d` installino dei file (ad esempio, `syslog` o `yast`).

Exempio 12.2: *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.

Nota

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.

Nota

12.2.4 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 (`info`) è il sistema ipertestuale di GNU™. Con `info info` otterrete delle prime istruzioni per l'uso. `info` è accessibile con Emacs `emacs -f info` o semplicemente con il comando `info`. Comodi da utilizzare sono tkinfo, xinfo; anche l'accesso tramite il sistema di aiuto risulta essere comodo.

12.2.5 Il comando ulimit

Con il comando `ulimit` *user limits*, potrete limitare l'accesso all'uso delle risorse del sistema o visualizzare le risorse. `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 12.1.

Tabella 12.1: *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, ad esempio, nell'autorizzare la creazione di quei core file necessari ai programmatori per il debug. L'utente non è in grado di aumentare i valori impostati dall'amministratore del sistema in `/etc/profile`; è però possibile inserire determinate impostazioni nel proprio `~/.bashrc`.

Exempio 12.3: *Impostazioni ulimit in /.bashrc*

```
# Limite della memoria reale:
ulimit -m 98304
```

```
# Limite della memoria virtuale:
ulimit -v 98304
```

La memoria viene espressa in KB. Per informazioni più dettagliate, consultate la pagina di manuale con `man bash`.

Nota

Non tutte le shell supportano le indicazioni `ulimit`. Se non potete fare a meno di questo tipo di restrizioni, PAM (p.es. `pam_limits`) offre ampie possibilità di impostazione.

Nota

12.2.6 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 sistema di gestione unitari della memoria *unified memory management*. Il motto di Linux è: *la memoria libera è cattiva memoria* *free memory is bad memory*, il che vuol dire che Linux cerca sempre di bilanciare le varie cache, ma di non lasciare mai della memoria del tutto inutilizzata.

Di per sé, il kernel non sa nulla di programmi o dati dell'utente, perché lui li amministra in cosiddette "Page Cache". Quando la memoria non basta più, parte di questi dati vengono spostati nella partizione swap o nei file dai quali sono stati originariamente estratti con la chiamata di sistema `mmap` (cfr. la pagina di manuale `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`.

12.2.7 Il file /etc/resolv.conf

La risoluzione del nome viene gestita tramite il file `/etc/resolv.conf`; cfr. la sezione 14.6 a pagina 339. 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.

12.2.8 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 per poter essere preconfigurato o adattato alle relative richieste in base a quanto stabilito dall'utente, amministratore di sistema e/o distribuzione.

Nella directory home viene installato per ogni utente il file di inizializzazione ~/.emacs di /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 questo file .gnu-emacs nella propria directory home e di editarlo lì:

```
cp /etc/skel/.gnu-emacs ~/.gnu-emacs
```

In .gnu-emacs il file ~/.gnu-emacs-custom viene impostato come custom-file; se l'utente vuole effettuare delle impostazioni proprie ricorrendo alle possibilità offerta da customize, esse saranno memorizzate sotto ~/.gnu-emacs-custom.

Con il pacchetto emacs nel caso di SUSE LINUX il file site-start.el viene installato 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 dei file di configurazione speciali, che vengono installati con i pacchetti aggiuntivi di Emacs della distribuzione (p. es. il pacchetto psgml); questo tipo di file di configurazione si trova anche sotto /usr/share/emacs/site-lisp ed iniziano sempre con suse-start-.

L'amministratore di sistema può effettuare nel file default.el delle impostazioni che avranno validità per tutto il sistema. Ulteriori informazioni su questo file solo reperibili nel file info su Emacs, nell' *Init File*: info:/emacs/InitFile. Lì viene anche descritto come evitare che questo file venga caricato – se dovesse rendersi necessario.

Le componenti di Emacs sono distribuiti su diversi pacchetti:

- Il pacchetto base emacs.

- In più di solito si deve installare il pacchetto `emacs-x11` che contiene il programma *con* supporto per l'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) etc.

12.3 Il boot con l'initial ramdisk

12.3.1 La problematica

Non appena il kernel di Linux è caricato e il file system root (`/`) è montato, possono venire eseguiti i programmi e caricati altri moduli del kernel che mettano a disposizione funzionalità supplementari. Il mount del file system root è tuttavia soggetto ad alcune premesse: per poter comunicare con il dispositivo su cui si trova il file system root (specialmente driver SCSI), il kernel ha bisogno dei driver corrispondenti. Inoltre, il kernel deve contenere il codice necessario per leggere il file system (`ext2`, `reiserfs`, `romfs` etc.). È anche possibile che il file system root sia già cifrato; in questo caso, per fare il mount, è necessaria la password/chiave.

Per quanto riguarda il problema dei driver SCSI, si può pensare a diverse soluzioni: il kernel può contenere tutti driver possibili e immaginabili. Il che non rende le cose più facili, dal momento che potrebbero verificarsi dei conflitti, ed inoltre gonfierebbero il kernel. Un'altra possibilità consiste nel mettere a disposizione diversi kernel che contengano solo uno o pochi driver SCSI. Anche questo metodo presenta delle difficoltà, poiché necessita di un gran numero di kernel differenti, ed in più la presenza di diversi kernel ottimizzati (ottimizzazione Pentium, SMP, etc.).

Caricare il driver SCSI come modulo porta alla questione generale risolta dal concetto dell'*initial ramdisk*: la possibilità di eseguire programmi user space già prima del mount del file system root.

12.3.2 Il concetto dell'initial ramdisk

L'*initial ramdisk* (denominato anche initdisk o initrd) risolve proprio questo tipo di problema. Il kernel di Linux consente di caricare un (piccolo) file system in una ramdisk ed eseguire lì dei programmi, prima che venga montato il file system root vero e proprio. Il caricamento dell'`initrd` viene svolto dal bootloader (GRUB, LILO etc.); tutti questi bootloader necessitano soltanto le routine del BIOS per caricare i dati dal dispositivo di caricamento. Una volta che il bootloader carica il kernel, potrà caricare anche l'initial ramdisk. In questo modo non sono necessari speciali driver.

12.3.3 Processo di caricamento con initrd

Il bootloader carica il kernel e `initrd` nella memoria e inizializza il kernel, comunicandogli che è disponibile un `initrd` e indicandogli la sua locazione nella memoria. Se `initrd` è compresso (e, generalmente, lo è), il kernel lo scompatta e lo monta come file system root temporaneo. A questo punto, nell'`initrd` viene inizializzato un programma dal nome linuxrc. Questo programma può svolgere tutte le funzioni necessarie a montare il vero file system root. Quando linuxrc ha concluso, l'`initrd` (temporaneo) viene "smontato" *unmounted* ed il processo di boot procedere con il montaggio del vero file system root. Il montaggio di `initrd` e l'esecuzione di linuxrc possono quindi venire considerati come un breve intermezzo durante una normale procedura di caricamento. Dopo il boot della partizione root, il kernel prova a montare `initrd` sulla directory `/initrd`. Se non ci riesce, ad esempio perché non trova un punto di mount `/initrd`, esso proverà a smontare `initrd`. Se non gli riesce neanche questo, il sistema continuerà a funzionare come al solito, ma la memoria occupata da `initrd` non verrà mai liberata e non potrà essere usata da nessun'altra componente del sistema.

Il programma linuxrc

Il programma linuxrc in `initrd` deve portare il nome `linuxrc` e trovarsi nella directory root di `initrd`. Inoltre, deve essere eseguibile solamente dal kernel. Ciò significa che linuxrc può senz'altro avere un link dinamico; in questo caso, le librerie condivise devono come al solito essere disponibili completamente sotto `/lib` in `initrd`. Inoltre linuxrc può essere anche uno script di shell, ragion per cui dovrà esserci una *shell* detta anche finestra di comando in `/bin`. In altre parole, `initrd` deve contenere un sistema Linux minimo che permetta l'esecuzione del programma linuxrc. All'installazione di SUSE LINUX, viene usato un linuxrc con un link statico, per

poter mantenere `initrd` il più piccolo possibile (lo spazio sui dischetti di boot non è illimitato). linuxrc viene eseguito con i privileggi di `root`.

Il vero file system root

Non appena linuxrc ha finito, `initrd` viene smontato e rimosso, il processo di boot continua normalmente con il kernel che monta il vero file system root. Cosa debba venire montato come file system root può essere determinato da linuxrc. linuxrc dovrà prima montare il file system `/proc` e scrivere il valore del vero file system root in forma numerica sotto `/proc/sys/kernel/real-root-dev`.

12.3.4 Bootloader

La maggioranza dei bootloader (soprattutto GRUB, LILO e syslinux) sono in grado di usare `initrd`. Ecco come istruire i singoli bootloader ad utilizzare un `initrd`:

GRUB immettere la riga seguente in `/boot/grub/menu.lst`:

```
initrd (hd0,0)/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`.

LILO immettere la seguente riga in `/etc/lilo.conf`:

```
initrd=/boot/initrd
```

Il file `/boot/initrd` è l'*initial ramdisk*. Esso può (ma non deve) essere compresso.

syslinux immettere la seguente riga in `syslinux.cfg`:

```
append initrd=initrd
```

La riga può contenere ulteriori parametri.

12.3.5 L'impiego di initrd con SUSE

Installazione del sistema

`initrd` viene usato già da parecchio tempo per l'installazione; se si esegue l'installazione manualmente l'utente può caricare moduli del kernel in linuxrc ed eseguire le impostazioni necessarie all'installazione. linuxrc inizializza poi YaST, che esegue l'installazione. Una volta che YaST abbia terminato il suo lavoro, comunica a linuxrc, dove trovare il file system root appena installato. linuxrc scrive questo valore in `/proc` ed esegue un reboot. In seguito si riavvia YaST e vengono installati i rimanenti pacchetti per il sistema appena installato.

Eseguire il boot del sistema installato

In passato, YaST metteva a disposizione per l'installazione più di 40 kernel, che si differenziavano uno dall'altro per il fatto che ognuno di essi conteneva un determinato driver SCSI. Ciò era necessario per poter montare il file system root dopo il caricamento. Altri driver potevano venire aggiunti in un secondo momento sotto forma di moduli.

Poiché, nel frattempo, esistono anche kernel ottimizzati, questo concetto non è più proponibile: ora sarebbero necessarie più di 100 immagini di kernel.

Pertanto, si usa un `initrd` ormai anche per il normale avvio del sistema. Il funzionamento è analogo a quello della installazione. Il linuxrc qui usato è però solo uno script di shell con l'unico compito di caricare determinati moduli. Si tratta, di norma, di un solo modulo; cioè di quel driver SCSI necessario per accedere al file system root.

Creare un initrd

La creazione di un `initrd` avviene tramite lo script `mkinitrd` (ex `mk_initrd`). In SUSE LINUX, i moduli da caricare vengono stabiliti tramite la voce `INITRD_MODULES` in `/etc/sysconfig/kernel`. Dopo un'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, carichiamo tutti i driver SCSI usati durante l'installazione tramite `initrd`.

Nota

Poiché il caricamento di `initrd` tramite il bootloader viene eseguito come il caricamento del kernel stesso (LILO annota nel suo file `mappa` la locazione dei file), dopo ogni modifica di `initrd`, si deve reinstallare il bootloader; se utilizzate GRUB questo non è necessario.

Nota

12.3.6 Possibili difficoltà – kernel auto-compilati

Se compilate un kernel spesso può subentrare il seguente problema: per abitudine, il driver SCSI viene linkato al kernel, senza modificare l'attuale `initrd`. Durante il boot avviene la seguente cosa: il kernel contiene di già il driver SCSI, l'hardware viene riconosciuto. `initrd` cerca però di caricare nuovamente il driver sotto forma di modulo; con alcuni driver SCSI (specialmente con `aic7xxx`), ciò porta all'arresto del sistema. A dire il vero, questo è un errore del kernel (un driver già esistente non dovrebbe venire caricato una seconda volta come modulo); il problema è però già noto in riferimento ai driver seriali.

Questo incoveniente può essere risolto in modi diversi: configurare il driver come modulo (in questo caso verrà caricato correttamente in `initrd`), o eliminare `initrd` da `/etc/lilo.conf` o rispettivamente da `/etc/grub/menu.lst` cosa che produce lo stesso effetto di eliminare il driver da `INITRD_MODULES` ed immettere `mkinitrd`, che, a sua volta, constaterà che non è necessario alcun `initrd`.

12.3.7 Prospettiva

In futuro è pensabile che `initrd` possa venire usato per molte più cose (e più complesse), non solo per caricare i moduli necessari all'accesso a `/`.

- File system root su software RAID (linuxrc imposta i dispositivi `md`)
- File system root su LVM
- File system root è cifrato, (linuxrc richiede la password)
- File system root su un disco rigido SCSI connesso a un adapter PCMCIA

Ulteriori informazioni

- `/usr/src/linux/Documentation/ramdisk.txt`
  (Disponibile solo se sono stati installati i sorgenti del kernel)
- La pagina di manuale di initrd.

12.4 linuxrc

linuxrc è un programma che viene inizializzato durante la fase di caricamento del kernel prima che venga fatto il boot. Questa proprietà del kernel permette di caricare un piccolo kernel modulare e, successivamente, i driver veramente necessari sotto forma di moduli. linuxrc vi aiuta a caricare i driver necessari per il vostro hardware. Normalmente, tuttavia, ci si può affidare tranquillamente all'identificazione automatica dell'hardware, eseguita da YaST prima dell'avvio. Potete utilizzare linuxrc sia per l'installazione, che 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 12.5 a pagina 284.

12.4.1 Menù principale

Dopo aver impostato la lingua e la tastiera, avrete accesso al menù principale di linuxrc (vedi Figura 1.2 a pagina 11). Di norma, si usa linuxrc per avviare Linux. Il nostro obiettivo è pertanto la voce 'Installazione/Avviare sistema'. Che riusciate ad accedere a questa voce direttamente o meno, dipende dall'hardware del PC e dalla portata dell'installazione; per un approfondimento, consultate il paragrafo 1.1 a pagina 8.

12.4.2 Impostazioni

Potete ora impostare la'Lingua', lo 'Schermo' (monocromatico o policromatico), 'Mappatura della tastiera' e 'Debug (Esperti)'.

12.4.3 Informazioni sul sistema

Sotto 'Informazioni sul sistema' (figura 12.1 nella pagina successiva) troverete, oltre ai messaggi del kernel, gli indirizzi I/O delle schede PCI, la capacità della memoria principale rilevata da Linux.

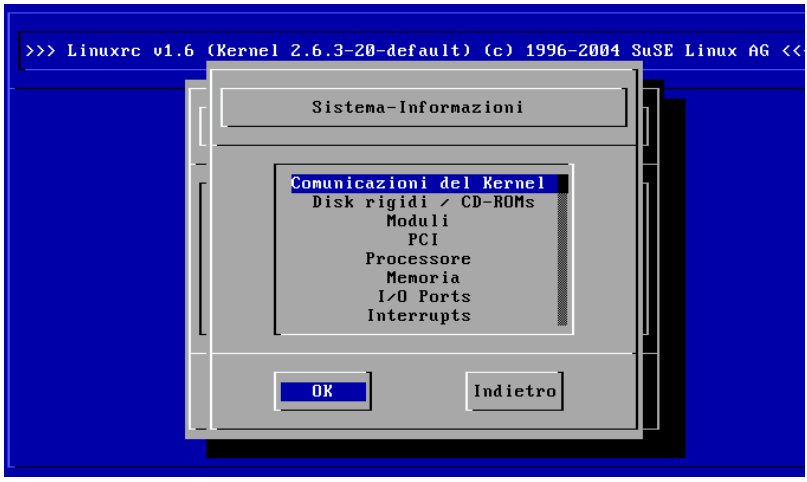

Figura 12.1: *Informazioni del sistema*

Il seguente esempio mostra il riconoscimento di un disco rigido e di un dispositivo CD-ROM connessi ad un adapter EIDE. In questo caso, per l'installazione non si ha bisogno dei moduli del kernel:

```
hda: ST32140A, 2015MB w/128kB Cache, LBA, CHS=1023/64/63
hdb: CD-ROM CDR-S1G, ATAPI CDROM drive
Partition check:
 hda: hda1 hda2 hda3 < hda5 >
```

Se avete inizializzato un kernel in cui sia già stabilmente integrato un driver SCSI, non sarà naturalmente più necessario caricare alcun modulo SCSI. Comunicazioni tipiche del riconoscimento di un adapter SCSI e dei dispositivi ad esso collegati sono:

```
scsi : 1 host.
Started kswapd v 1.4.2.2
scsi0 : target 0 accepting period 100ns offset 8 10.00MHz FAST SCSI-II
scsi0 : setting target 0 to period 100ns offset 8 10.00MHz FAST SCSI-II
  Vendor: QUANTUM   Model: VP32210           Rev: 81H8
  Type:   Direct-Access                      ANSI SCSI revision: 02
Detected scsi disk sda at scsi0, channel 0, id 0, lun 0
scsi0 : target 2 accepting period 236ns offset 8 4.23MHz synchronous SCSI
scsi0 : setting target 2 to period 248ns offset 8 4.03MHz synchronous SCSI
  Vendor: TOSHIBA   Model: CD-ROM XM-3401TA  Rev: 0283
  Type:   CD-ROM                             ANSI SCSI revision: 02
scsi : detected 1 SCSI disk total.
SCSI device sda: hdwr sector= 512 bytes. Sectors= 4308352 [2103 MB] [2.1 GB]
Partition check:
 sda: sda1 sda2 sda3 sda4 < sda5 sda6 sda7 sda8 >
```

12.4.4 Caricare i moduli

Scegliete i moduli (driver) di cui avete bisogno. linuxrc vi mostrerà un elenco dei driver disponibili. Sulla sinistra avrete il nome del modulo, sulla destra una breve descrizione dell'hardware per cui è necessario il modulo. Per alcune componenti vi sono a volte diversi driver o nuovi driver alfa.

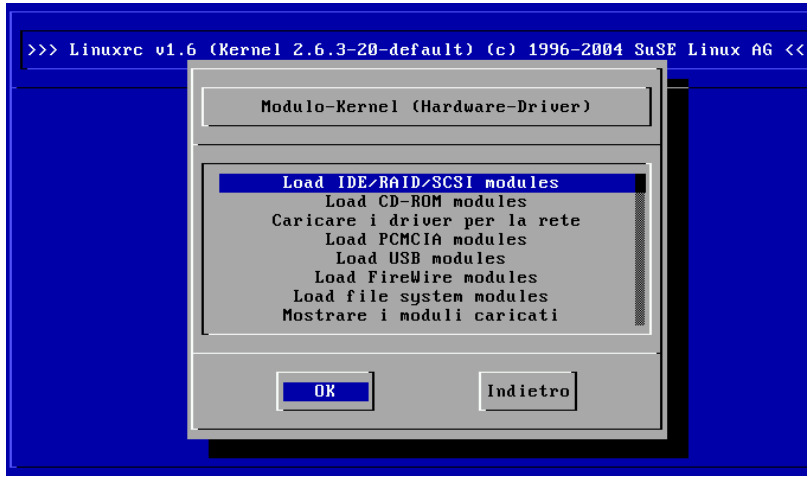

Figura 12.2: *Caricare i moduli*

12.4.5 Inserimento dei parametri

Una volta individuato il driver richiesto per il vostro hardware, premete (Return). A questo punto appare una maschera in cui poter digitare i parametri del modulo da caricare. Ricordiamo che, al contrario del prompt del kernel, qui più parametri per uno stesso modulo devono essere separati da uno spazio.

In molti casi non è necessaria l'esatta specificazione dell'hardware; la maggior parte dei driver individua da sè i suoi componenti. Solo schede di rete e lettori di CD-ROM un pò datati con propria scheda controller potrebbero necessitare dei parametri. In ogni caso, provate prima con (Return).

Con alcuni moduli, il riconoscimento e l'inizializzazione dell'hardware può durare un pó. Passando alla console virtuale 4 ((Alt) + (F4)), potrete leggere i messaggi che vengono visualizzati in fase di caricamento del kernel. Gli

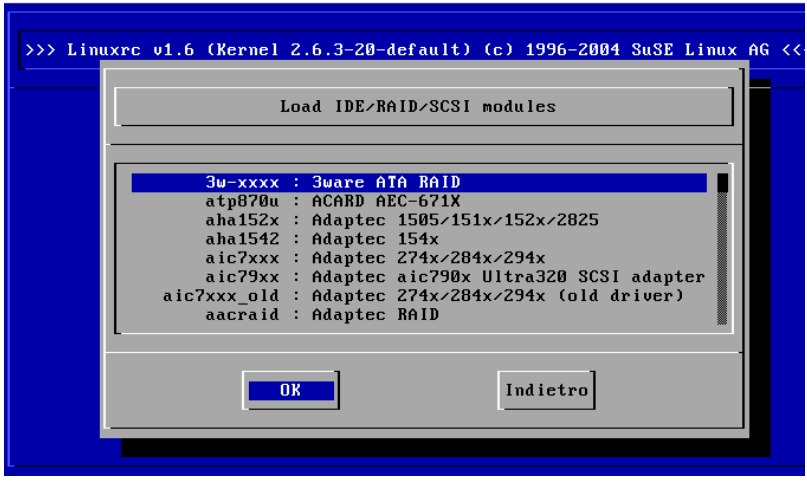

Figura 12.3: *Scelta dei driver per SCSI*

adapter SCSI sono piuttosto lenti, poiché aspettano che tutti i dispositivi collegati siano stati identificati.

Se il caricamento del modulo ha funzionato, linuxrc vi mostra i messaggi del kernel, di modo che possiate assicurarvi che tutto sia andato bene; in caso contrario, i messaggi vi permetteranno di trovare la causa dell'errore.

12.4.6 Inizializzare il sistema / l'installazione

Una volta che abbiate ottenuto il supporto del kernel per il vostro hardware, potete passare al punto 'Inizializzare il sistema / l'installazione'. Da qui potete inizializzare diversi processi: 'Avviare installazione/update', 'Caricare sistema installato' (la partizione root deve essere nota), 'Inizializzare sistema di salvataggio' (vd. sezione 12.5 a pagina 284) e 'Espelli CD'.

Se avete fatto il boot da un cosiddetto 'LiveEval-CD', avrete ora anche la voce "Inizializzare il LiveEval-CD". Potete scaricare delle immagini ISO dal server FTP (`live-eval-<VERSIONE>`): `ftp://ftp.suse.com/pub/suse/i386/`.

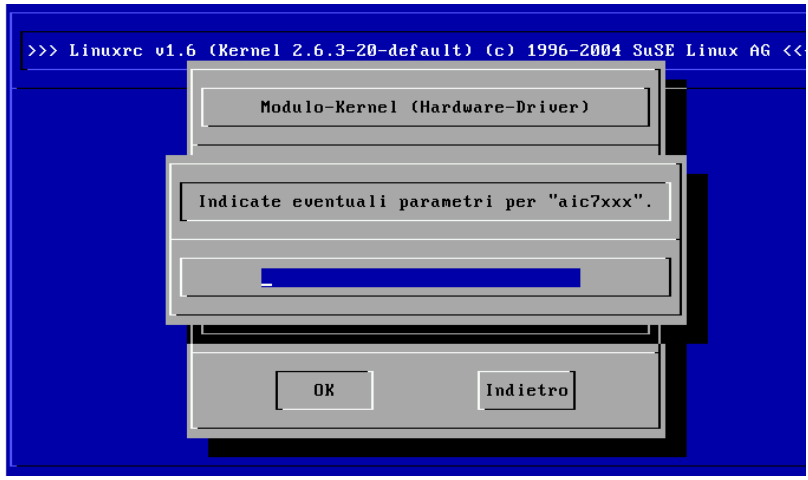

Figura 12.4: *Digitazione dei parametri per il caricamento dei moduli*

Nota

La voce 'Inizializzare il Live-CD' vi permette di eseguire un test per verificare la compatibilità del computer o portatile, *senza* dovere eseguire l'installazione sul disco rigido.

Nota

Per l'installazione (figura 12.5 nella pagina successiva), come anche per il sistema di salvataggio, potete scegliere tra diversi dispositivi (Figura 12.6 a pagina 285).

12.4.7 Passare dei parametri a linuxrc

Se non linuxrc non si trova nel modo manuale, esso cercherà un file info o 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 `/linuxrc.config` che verrà caricato come primo. Comunque si consiglia di eseguire delle modifiche nel file info.

Un file info è composto da parole chiave e rispettivi valori: `key: value`. Queste coppie di chiave/valori possono essere passati in questa forma anche al prompt del kernel. Un elenco dei valori possibili è reperibile nel file

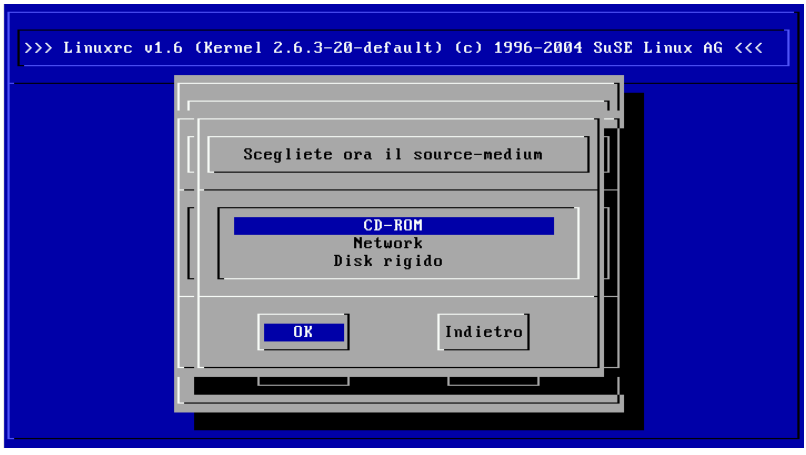

Figura 12.5: *Scelta del dispositivo d'installazione in linuxrc*

`/usr/share/doc/packages/linuxrc/linuxrc.html`. Ecco alcuni di rilievo:

- Install: URL (nfs, ftp, hd, ...)
- HostIP: 10.10.0.2
- Proxy: 10.10.0.1
- Netdevice: eth0
- Textmode: 0 | 1
- AutoYast: ftp://autoyastfile
- VNC: 0 | 1
- VNCPassword: password
- UseSSH: 0 | 1
- SSHPassword: password
- ForceInsmod: 0 | 1 (utilizzare l'opzione `-f`, se viene invocato `insmod`).
- Insmod: parametro del modulo

- AddSwap: 0|3|dev/hda5

  Con 0 non é richiesta una `swap`, nel caso di un numero positivo, viene abilitata la partizione del numero indicato; potete anche indicare il nome della partizione.

12.5 Il sistema di salvataggio 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. Inoltre vi è un CD di SUSE LINUX atto al boot (il *LiveEval-CD*), che può fungere da sistema di salvataggio. Sono diverse utility che fanno parte del sistema di salvataggio con il quale potrete risolvere dei problemi dovuti ad hard disk a cui non riuscite più ad accedere, file di configurazione corrotti etc. Parted (`parted`) fa parte del sistema di salvataggio che vi permette di modificare le dimensioni delle partizioni. In caso di necessità il sistema di salvataggio può essere lanciato anche manualmente se non volete ricorrere al resizer integrato in YaST. Delle informazioni su Parted sono reperibili all'indirizzo:

`http://www.gnu.org/software/parted/`

12.5.1 Lanciare il sistema di salvataggio

Il sistema di salvataggio viene avviato da un CD o DVD. La premessa è che il lettore di CD/DVD sia atto al boot; se necessario dovete modificare la sequenza di avvio nel BIOS.

Ecco come inizializzare il sistema di salvataggio:

1. Inserite il primo CD o DVD di SUSE LINUX nel lettore ed accendete il vostro sistema.
2. Potete eseguire il boot completo o selezionare la voce 'Installazione manuale' e specificare se necessario accanto a 'boot option' determinati parametri di boot.
3. Impostate in linuxrc la lingua e mappatura della tastiera.
4. Ora potete caricare i moduli del kernel richiesti dal vostro sistema. Caricate *tutti* i moduli di cui credete che siano necessari per il sistema di salvataggio. Il sistema di salvataggio per ragioni di spazio ne contiene solo pochi.

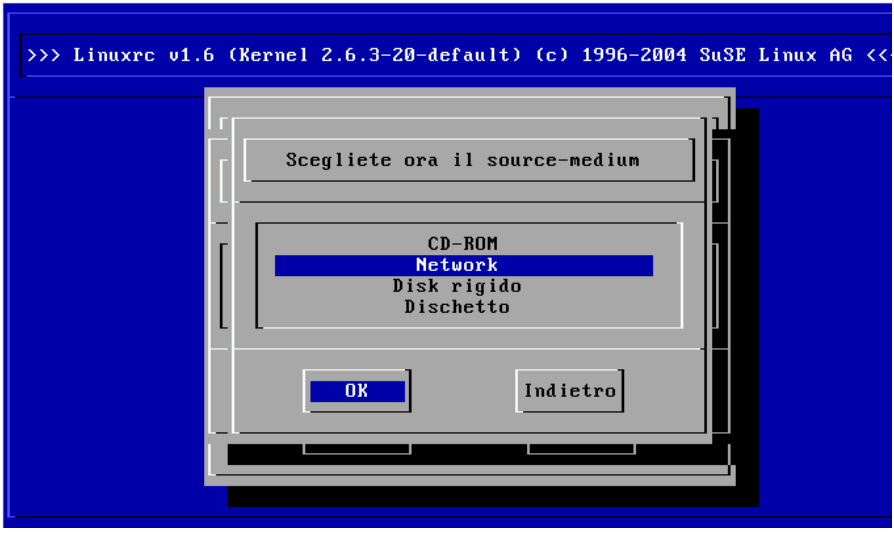

Figura 12.6: *Il mezzo sorgente del sistema di salvataggio*

5. Selezionate nel menu principale la voce 'Avvia installazione/sistema'.
6. Nel menù 'Inizializzare l'installazione/il sistema', scegliete il punto 'Inizializzare il sistema di salvataggio' (vd. figura 1.3 a pagina 13) e indicate il dispositivo sorgente desiderato (figura 12.6).

   'CD-ROM': viene utilizzato il sistema di salvataggio sul CD-Rom.

   'Rete': Il sistema di salvataggio viene avviato via rete. In questo caso dovrà essere caricato il modulo del kernel per la scheda di rete; cfr. le indicazioni generali nel paragrafo 1.3.2 a pagina 17 . In un sottomenù, troverete una serie di protocolli (vd. fig. 12.7 nella pagina seguente): NFS, FTP, SMB, ecc.

   'Disco rigido': Se avete copiato il sistema di salvataggio su di un disco rigido che attualmente è indirizzabile, potete indicare qui dove risiede il sistema di salvataggio che in tal modo potrete utilizzare.

Indipendentemente dal dispositivo scelto: il sistema di salvataggio viene decompresso, caricato, montato ed inizializzato in una ramdisk quale nuovo file system root. Ora è pronto per l'uso.

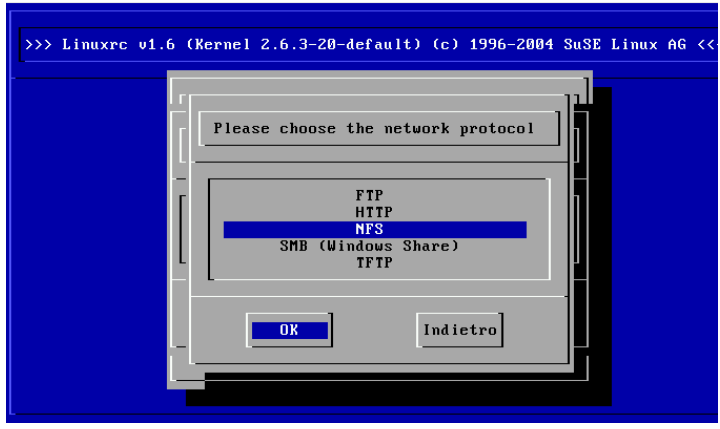

Figura 12.7: *Protocolli di rete*

12.5.2 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 con cui potrete eseguire il login come utente `root` senza la password. Con (Alt) + (F10) andate alla console del sistema che contiene le comunicazioni del kernel e syslog.

Sotto `/bin` trovate la shell detta anche finestra di comando e utility (p.es. mount). Importanti utility di file e di rete per controllare e riparare file system come e2fsck, si trovano sotto `/sbin`. In `/sbin` avete anche i file binari più importanti per l'amministrazione del sistema come fdisk, mkfs, mkswap, init, shutdown, e per la rete, come ifconfig, route e netstat. Come editor vi è vi che trovate sotto `/usr/bin`; qui troverete anche altri tool: (grep, find, less etc.) come pure il programma telnet.

Accesso al sistema normale

Per montare il vostro sistema SUSE LINUX sul disco rigido, vi è il punto di mount `/mnt`; naturalmente, per i vostri scopi, potete creare altre directory e usarle come punto di mount.

Supponiamo, per esempio, che `/etc/fstab` vi indica che il vostro sistema si presenta come il file-esempio 12.4.

Exempio 12.4: *Esempio /etc/fstab*

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

Attenzione

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

Attenzione

Per avere accesso al vostro sistema, eseguite il mounti 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 errori nei file di configurazione come `/etc/fstab`, `/etc/passwd`, `/etc/inittab` (che naturalmente ora si trovano 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. Ciò può avvenire dopo uno spegnimento non corretto (per esempio a causa di una mancanza di corrente) o dopo un crollo del sistema. I file system non possono venire riparati durante il normale funzionamento del sistema. In presenza di danni gravi, potrebbe non essere possibile montare il file system root e l'avvio del sistema causare un `kernel panic`. L'unica cosa da fare a questo punto, 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 e2fsck e, per la diagnosi, dumpe2fs. Con essi avrete la meglio sulla maggior parte dei problemi. Poiché, in caso di emergenza, non avrete più accesso neanche alla pagina di manuale di e2fsck, la trovate annessa nell'appendice C a pagina 557.

Esempio: se un file system, a causa di un *Superblocco non valido* non si lascia più montare, molto probabilmente, in un primo tempo, fallirà anche

`e2fsck`. La soluzione consiste nell'usare uno dei backup del superblocco creati nel file system ogni 8192 blocchi (8193, 16385...). Ciò viene eseguito p.es. con il comando:

```
e2fsck -f -b 8193 /dev/<partizione_difettosa>
```

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 tutto sia a posto.

12.6 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.

Nel modo di testo sono a disposizione 6 console virtuali; premendo la combinazione di tasti Alt+F1 - 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-F6. Con Alt+F7 ritornate a X11.

12.7 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 leggono `terminfo`, o i cui file di configurazione sono stati modificati direttamente (`vi`, `less` etc.). Altre applicazioni non-SUSE devono venire adattate a queste impostazioni di default.

In X il tasto compose (Multi_key) si ha tramite la combinazione di tasti Ctrl + Shift (destro); cfr. la registrazione in `/usr/X11R6/lib/X11/Xmodmap`.

Per il cinese, giapponese o coreano (CJK) consultate il sito allestito da Mike Fabian: `http://www.suse.de/~mfabian/suse-cjk/input.html`.

12.8 Adattamenti locali – I18N/L10N

SUSE LINUX è internazionale e può venire adattato alle condizioni locali;. cioè, 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 per la superficie e le comunicazioni dei programmi (*native language support*), ma anche delle categorie per le *messaggi* (lingua), *classi dei caratteri*, *sequenza della classificazione*, *data e ora*, *numeri* e *valuta*. Ognuna di queste categorie può venire stabilita direttamente tramite una propria variabile o indirettamente tramite una variabile superiore nel file `language` (vedi la pagina di manuale `man locale`):

1. `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`.

2. `RC_LC_ALL`: questa variabile sovrascrive, se configurata, i valori della variabile nominata nel punto 1.

3. `RC_LANG`: questo è il cosiddetto fallback, nel caso che nessuna delle suddette variabili sia stata configurata; come standard, SUSE LINUX imposta `RC_LANG`; in questo modo, l'utente può immettere più facilmente propri valori.

4. `ROOT_USES_LANG`: è una variabile `yes/no`. Se è impostata su `no`, `root` lavora sempre nell'ambiente POSIX.

Le variabili vanno impostate tramite l'editor `sysconfig`. Il valore di tali variabili è composto dall'indicazione della lingua *language code*, paese o territorio *country code*, set dei caratteri *encoding* e l'opzione *modifier*. Le singole indicazioni vengono collegate con caratteri speciali:
LANG=⟨*language*⟩[[_⟨*COUNTRY*⟩].⟨*Encoding*⟩[@⟨*Modifier*⟩]]

12.8.1 Esempi

Impostate sempre lingua e nazione assieme. 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 definiti in ISO 3166 (`http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html`). Logicamente, possono venire scelti solo i valori per il file di descrizione utilizzabili che si trovano sotto `/usr/lib/locale`. Altri file di descrizione possono venire creati con l'aiuto di `localedef` preso dai file in `/usr/share/i18n`.

`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. supportata dall'editor Emacs.

`LANG=it_IT@euro` Segue un esempio per settare una opzione (`euro`).

SuSEconfig legge le variabili in `/etc/sysconfig/language` e scrive le indicazioni su `/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 soprascrivere 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`

12.8.2 Adattamento per il supporto della lingua

Generalmente, per ottenere un fall back, i file delle categorie *Messaggi* vengono archiviati solo nella directory della lingua (p.e. `de`). Se quindi `LANG` viene impostato su p.es. `it_CH` e se il file Message non è esistente sotto `/usr/share/locale/it_CH/LC_MESSAGES`, si ricorre a `/usr/share/locale/it/LC_MESSAGES`.

Con `LANGUAGE` è anche possibile determinare una cascata di fallback; p.es. per il bretone -> francese o per il gallego -> spagnolo -> portoghese:

```
LANGUAGE="br_FR:fr_FR"
```

```
LANGUAGE="gl_ES:es_ES:pt_PT"
```

O per ricorrere a varianti del norvegese nynorsk o 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.

Problemi possibili

Il punto decimale in cifre del tipo 1.000 non viene riconosciuto. Probabilmente `LANG` si trova su `it`. Poiché la descrizione alla quale ricorre la glibc si trova in `/usr/share/locale/it_IT/LC_NUMERIC`, `LC_NUMERIC` deve venire impostato su `it_IT`.

Ulteriori informazioni:

- *The GNU C Library Reference Manual*, capitolo. “Locales and Internationalization”; contenuto nel `glibc-info`.
- Jochen Hein, sotto il lemma “NLS”.
- *German-Howto* di Winfried Trümper `file:/usr/share/doc/howto/en/html/German-HOWTO.html`
- 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`.
- *Supporto di CJK in SuSE Linux* in inglese redatto da Mike Fabian `http://www.suse.de/~mfabian/suse-cjk/suse-cjk.html`.

Il concetto di boot

Caricare ed inizializzare un sistema Unix non è una banalità neanche per amministratori di sistema esperti. Questo capitolo vi introduce brevemente il concetto di caricamento di SUSE LINUX che mette in pratica inizializzazione del sistema secondo la specificazione LSB (versione 1.3.x); (cfr. la sezione 12.1.1 a pagina 266).

Con la frase lapidaria “Uncompressing Linux...”, il kernel assume il controllo di tutto l’hardware del sistema. Esso verifica ed imposta la console (ovvero la sezione del BIOS delle schede grafiche ed il formato di output dello schermo), per poi leggere i parametri del BIOS ed inizializzare le interfacce elementari della scheda madre. In seguito, i driver (che fanno comunque parte del kernel) esaminano l’hardware disponibile ed eventualmente lo inizializzano. Dopo la verifica delle partizioni ed il mount del file system "root", il kernel avvia il programma init. Con init, viene a sua volta avviato il sistema vero e proprio, con i rispettivi programmi di servizio e configurazione. Sarà poi il kernel a gestire tutto il sistema: controllerà il tempo di elaborazione dei singoli programmi, metterà a disposizione la memoria necessaria e gestirà l’accesso all’hardware.

13.1 Il programma init

Il programma init è il processo che si occupa dell’inizializzazione corretta del sistema. Lo si potrebbe definire “il padre di tutti i processi” del sistema.

Tra tutti i programmi, init è quello che svolge un ruolo davvero particolare: init viene avviato direttamente dal kernel ed è immune al segnale 9, con il quale potete “freddare” ogni processo. Tutti gli altri processi vengono avviati da init stesso o da uno dei suoi processi “figli”.

init si configura centralmente, tramite il file `/etc/inittab`, nel quale potrete definire i cosiddetti runlevel (vd. la sezione, 13.2) e stabilire quali servizi e demoni debbano essere disponibili nei singoli runlevel ovvero livelli di esecuzione del sistema. A seconda dei parametri in `/etc/inittab`, init avvia i relativi script, che per motivi di praticità sono stati tutti raccolti nella directory `/etc/init.d`.

L’avvio del sistema (e, chiaramente, anche lo spegnimento) spetta quindi unicamente al processo di init. Il kernel può dunque essere visto come un processo di fondo, il cui compito consiste nel gestire i processi avviati, assegnare loro un tempo di elaborazione e di gestire l’accesso all’hardware.

13.2 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 (vd. la tabella 13.1). Alternativamente, potrete impostare il runlevel desiderato durante il caricamento (ad esempio al prompt di boot); il kernel passerà i parametri che non elaborerà direttamente al processo init senza modificarli.

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 `shutdown now` 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.

Nota

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.

Nota

Tabella 13.1: *Elenco dei livelli di esecuzione sotto Linux*

Runlevel	Significato
0	Arresto del sistema (ingl.*System halt*)
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* cioè 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 (standard), GDM o XDM (ingl.*Full multiuser with network and xdm*)
6	Riavvio del sistema (ingl. *System reboot*)

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 l' Sistema X Window sia già stato configurato correttamente ; (vd. capitolo 4 a pagina 77). Verificate se il sistema funziona come lo desiderate immettendo in seguito `init 5`. In caso affermativo, con YaST potete impostare il runlevel di default su `5`.

Attenzione

Personalizzare /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 ai 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. Dopo il boot, ripristinate quindi la copia di backup con il comando `cp`.

Attenzione

13.3 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 avvio* 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:

- L'amministratore (`root`) ordina al processo init di cambiare runlevel, immettendo `init 5`.

- 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.
- 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.

  Nota

  Gli script di arresto iniziano sempre con K (ingl. *kill*), mentre gli script di avvio iniziano con S (ingl. *start*).

  Nota

- 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).

13.4 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).
- 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 13.2.

Tabella 13.2: *Rassegna delle opzioni degli script init*

Opzione	Significato
`start`	Avviare servizio
`stop`	Fermare servizio
`restart`	Fermare e riavviare servizio, se il servizio era già in esecuzione; 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 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 (ovv. del link `/usr/lib/lsb/install_initd`) durante l'installazione o disinstallazione dei pacchetti del caso; cfr. la pagina di manuale di insserv.

Segue una breve descrizione dei primi script di caricamento e spegnimento, nonché degli script di controllo:

`boot` Viene eseguito allo 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`, attivato blogd (ingl. "Boot Logging Daemon") e, dopo l'installazione di un nuovo sistema o 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 oppure 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 con `man blogd`.

A questo script è allocata anche la directory `/etc/init.d/boot.d/`; tutti gli script di questa directory che comincino con la lettera `S` vengono automaticamente eseguiti all'avvio del sistema. Si verificano i file system, vengono eliminati tutti i file superflui sotto `/var/lock/` e configurata la rete per il dispositivo di loopback, se previsto. Inoltre viene impostata l'ora del sistema.

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 forse 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 all'entrata nel runlevel 0 o 6. Viene avviato sotto il nome `halt` o `reboot`. A seconda di come 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.

13.4.1 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 di `init`, `init.d` e `insserv`. In questo contesto sono di sicuro interesse anche le pagine di manuale di `startproc` e `killproc`.

Attenzione

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 13.2 a pagina 294.

Attenzione

- Se per un vostro programma o un vostro servizio (ingl. *service*) create un script di inizializzazione, utilizzate come modello il file `/etc/init.d/skeleton`. Salvate questo file sotto 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 per eseguire in modo corretto il comando di inizializzazione.
- Editate il blocco obbligatorio `INIT INFO` all'inizio del file:

Exempio 13.1: *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 ; vd. la sezione 13.5 .

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.

13.5 L'editor dei runlevel editor di YaST

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 13.1 a pagina 295. I servizi e demoni si abilitano o disabilitano in questa tabella che vi offre delle informazioni riguardanti i

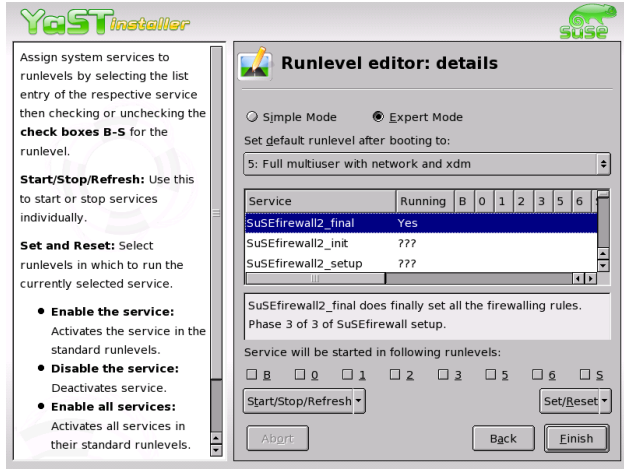

Figura 13.1: *YaST: editor dei runlevel*

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 'Avvia/Arresta/Aggiornare', decidete se utilizzare un determinato servizio. Con 'Aggiorna lo stato', potete verificare lo stato attuale, nel caso in cui 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.

Attenzione

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.

Attenzione

13.6 SuSEconfig e /etc/sysconfig

Principalmente la configurazione di SUSE LINUX viene realizzata tramite i file di configurazione che trovate sotto `/etc/sysconfig/`. Nelle versioni precedenti di SUSE LINUX si editava a riguardo il file `/etc/rc.config/` che è diventato ormai obsoleto. Quando installate SUSE LINUX 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.

I file in `/etc/sysconfig/` vengono usati solo da alcuni script in situazioni ben determinate. In questo modo si assicura che le impostazioni della rete vengano elaborate solo dagli script della rete e non da altri. Inoltre, molti altri file di configurazione del sistema vengono generati in dipendenza dai file sotto `/etc/sysconfig/`; cosa a cui è preposto SuSEconfig. Ad esempio, dopo una modifica della configurazione di rete, viene ricreato il file `/etc/host.conf`, dal momento che dipende dal tipo di configurazione.

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 attualizzerà tutti i file interessati.

Questo sistema rende possibile apportare delle rilevanti modifiche alla configurazione del computer senza dover per questo riavviarlo. 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`, vengono riavviati i programmi di rete appena modificati.

Per configurare il sistema vi consigliamo di procedere come segue:

- Portate il sistema nel *modo utente singolo*, ovvero (runlevel 1) con: `init 1`
- Modificate i file di configurazione. Servitevi a riguardo di un editor di testo o, meglio, dell'editor Sysconfig di YaST; cfr. la sezione 13.7 nella pagina successiva.

Attenzione

Editare manualmente la configurazione del sistema

Se *non* editate i file di configurazione che trovate sotto `/etc/sysconfig/` con YaST immettete un parametro vuoto seguito da due virgolette susseguenti (ad esempio `KEYTABLE=""`) e non dimenticate le virgolette all'inizio e alla fine di parametri che contengono degli spazi. Le variabili composte da una sola parola non necessitano delle virgolette.

Attenzione

- Eseguite SuSEconfig per rendere effettive le modifiche fatte. Questo avverrà automaticamente, se avete usato YaST per impostare il runlevel.
- 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.

Nota

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.

Nota

13.7 L'editor sysconfig di YaST

Nella directory`/etc/sysconfig`, troverete tutti i file contenenti le impostazioni principali per SUSE LINUX. L'editor sysconfig di YaST 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.

Attenzione

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.

Attenzione

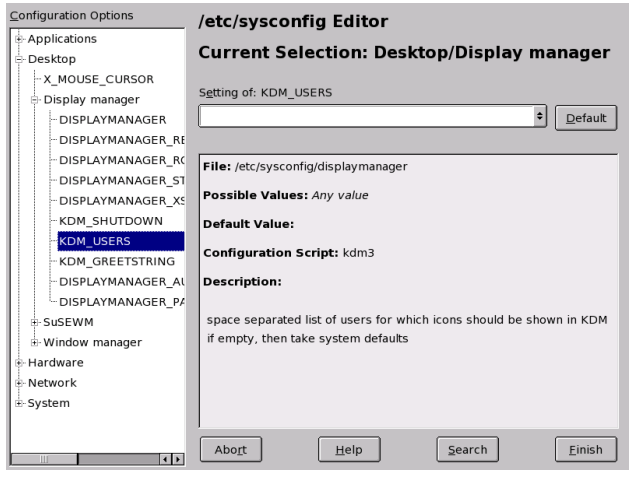

Figura 13.2: *YaST: configurazione del sistema tramite l'editor Sysconfig*

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.

Parte IV

Rete

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 sotto SUSE LINUX e l'aiuto di YaST l'accesso alla rete utilizzando una scheda di rete. Parleremo dei file centrali di configurazione e verranno illustrati alcuni dei tool principali. Dato che la configurazione di una rete può assumere diversi gradi di complessità, in questo capitolo descriveremo solo i meccanismi di base.

Anche la connessione ad Internet tramite PPP e modem, ISDN o DSL può essere comodamente configurata con YaST. Vd. il *manuale dell'utente*.

14.1 TCP/IP: il protocollo usato da Linux

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*; si tratta di 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/`. Nel frattempo, il protocollo TCP/IP è stato migliorato, ma il "nocciolo" del protocollo è rimasto invariato dal 1981.

Nota

I documenti RFC spiegano la struttura dei protocolli Internet. Se volete approfondire le vostre conoscenze su un determinato protocollo, i documenti RFC sono la fonte giusta. `http://www.ietf.org/rfc.html`

Nota

I servizi riportati nella tabella 14.1, consentono lo scambio di dati fra due computer Linux tramite TCP/IP:

Tabella 14.1: *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 garantita l'esatta sequenza dei dati, e può verificarsi la perdità 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 errori, ed è in grado di controllare il comportamento dei computer che partecipano alla 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 computer che usano il multicast IP. Purtroppo, in questa sede non possiamo entrare nei dettagli del multicasting IP.

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. La grandezza del pacchetto TCP/IP viene limitata 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.

14.1.1 Modello a strati

Tramite IP *Internet protocol* si ha una trasmissione di dati non garantita. TCP *Transmission control protocol* è in un certo senso un sopralzo del sottostante IP, per realizzare una trasmissione garantita dei dati. IP a sua volta non è altro che un sopralzo del protocollo sottostante che dipende dall'hardware, p.e Ethernet. Così si parla di modello a strati. A riguardo, osservate anche la figura 14.1 nella pagina successiva.

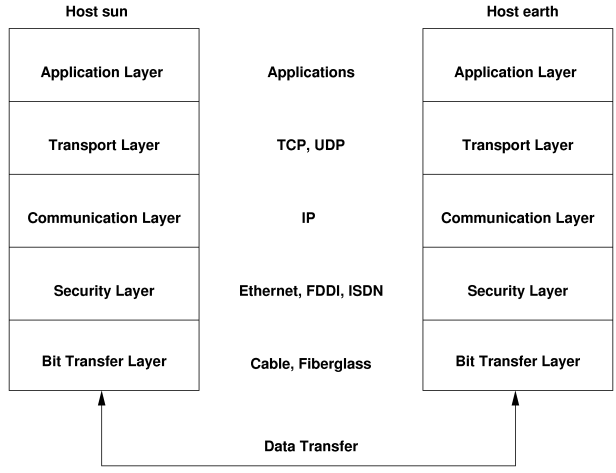

Figura 14.1: *Modello a strati semplificato per TCP/IP*

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.e. Ethernet) viene simboleggiata dallo strato di trasmissione dei bit e dallo strato di sicurezza.

- Mentre lo strato 1 è relazionato al tipo di cavi, ai tipi e codifica di segnale e cose simili, lo strato 2 regola il procedimento di accesso (quale computer può inviare dei dati e quando?) e la correzione degli errori (sicurezza dei dati, ecco perché *strato di sicurezza*). Lo strato 1 viene chiamato anche *strato di trasmissione dei bit*.
- Lo strato 3 a sua volta, *strato di mediazione* è responsabile per la trasmissione dei dati su lunghe distanze. Lo strato di mediazione, assicura che i dati arrivino al ricevente giusto.
- Lo strato 4, lo *strato di trasporto*, si occupa dei dati dell'applicazione: assicura che i dati arrivino a destinazione nella sequenza giusta, e che non vada perso niente. Lo strato di sicurezza controlla solo che i dati in entrata siano corretti. Lo *strato di trasporto* evita la perdita di dati.

- Nello strato 5 infine, si ha l'elaborazione dei dati tramite l'applicazione stessa.

Affinché ogni strato possa adempiere ai suoi compiti, devono venire aggiunte determinate informazioni al pacchetto di dati dallo strato corrispondente. Ciò avviene nell'*header*, l'intestazione del pacchetto di dati. Ognuno degli strati aggiunge, all'inizio del pacchetto in via di formazione, un piccolo blocco di dati, la cosiddetta testata del protocollo (ingl.*protocol header*). Se osserviamo un qualsiasi pacchetto di dati TCP/IP in viaggio su un cavo Ethernet, vediamo che è composto come rappresentato nella figura 14.2.

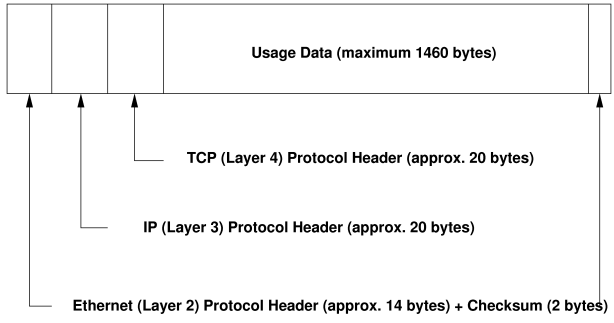

Figura 14.2: *Pacchetto TCP/IP nell'Ethernet*

Come vedete, il mondo non è ancora perfetto e, soprattutto, non privo di eccezioni. La somma di controllo dello stato di sicurezza si trova alla fine del pacchetto e non all'inizio: la cosa, però, è una semplificazione per l'hardware di rete. In un pacchetto, la quantità massima possibile dei dati utente (per quello che riguarda la rete Ethernet) è di 1460 byte.

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). Ognuno degli strati, deve preparare 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 al contrario; 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.

14.1.2 Indirizzi IP e routing

Nota

Nei seguenti paragrafi diamo una descrizione di reti IPv4. Per avere delle informazioni riguardanti IPv6 consultate la sezione 14.2 a pagina 318.

Nota

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 della tabella 14.1:

Exempio 14.1: *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 lungo 48 bit, univoco in tutto il mondo e memorizzato permanentemente 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, ma che sono stati assegnati più o meno casualmente, e quindi non sono adatti all'indirizzamento di host remoti. L'indirizzo *MAC* occupa però un ruolo di primo piano nella comunicazione tra gli host in una rete locale (ed è parte 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*).

Maschere di rete e routing

Poiché, in un primo tempo, il computer con l'indirizzo IP 192.168.0.0 non può sapere dove trovare il computer con l'indirizzo IP 192.168.0.20, si escogitò la maschera rete.

Detto in parole povere, in un computer con indirizzo IP, la (sotto)maschera di rete definisce che cosa si trova "dentro" e cosa si trova "fuori" la rete locale. I computer che si trovano "dentro" (in gergo "nella stessa sottorete") possono essere indirizzati direttamente; quelli "fuori" ("che non sono nella stessa sottorete") 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 (vd. tabella 14.2). Di regola, se sono disponibili più interfacce di rete, vengono controllati tutti i possibili indirizzi di invio.

I risultati dei collegamenti AND vengono confrontati. Se i risultati sono esattamente concordanti, vuol dire che il computer meta si trova nella stessa sottorete, in caso contrario esso dovra essere indirizzato tramite un gateway. Ciò significa che più bit "1" si trovano nella maschera di rete, meno computer possono venire indirizzati direttamente, dunque si dovrà passare per un gateway. A scopo esplicativo abbiamo elencato alcuni esempi nella tabella 14.2.

Exempio 14.2: *Congiunzione dell'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 spazi di indirizzi debbano essere raggiungibili tramite quale interfaccia di rete.

Per esempio, di solito tutti i computer 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 computer continuano ad essere indirizzabili in modo diretto.

Ethernet, anche se vantaggioso da un punto di vista di costo, non è indicato per coprire distanze lunghe, e dunque sarete costretti ad inoltrare i pacchetti IP tramite un altro tipo di hardware (p.e. 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 adatto 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 14.2: *Indirizzi speciali*

Tipo di indirizzo	**Descrizione**
Indirizzo base della rete	Si tratta dell'indirizzo della maschera di rete ed di un indirizzo qualsiasi preso dalla rete: cioè ciò che è raffigurato nella tabella 14.2 nella pagina precedente sotto `Risultato`. Questo indirizzo non può venire assegnato ad alcun computer.
L'indirizzo broadcast	Vuol dire: "contatta tutti i computer in questa sottorete". Per crearlo, si inverte in modo binario l'indirizzo della maschera di rete e collegato 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 un 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 sul proprio computer.

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:

Tabella 14.3: *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`

14.1.3 DNS – Domain Name System

Grazie al DNS (Domain Name System) non dovete necessariamente ricordarvi gli indirizzi IP: con l'aiuto di 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 computer 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 dipendente dalla gerarchia degli indirizzi IP sopra descritta.

Osserviamo da più vicino un nome completo, p.e. `laurent.suse.de` scritto nel formato `hostname.dominio`. Un nome completo (in gergo "Fully qualified domain name" o *FQDN*) è composto dal nome del computer accompagnato dal dominio. Il dominio si compone di una parte liberamente scelta (nel nostro esempio: `suse` e di un cosiddetto *top level domain*, *TLD*.

L'attribuzione dei TLD è un po' intricata. In America vengono p.e. usati TLD formati 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.e. `.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 computer 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 ad altri server dei nomi le richieste a lui inoltrate.

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`.

Affinché il vostro computer sia in grado di risolvere un nome in un indirizzo IP, deve conoscere 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.

DNS non risolve solo dei nomi di host, sa fare di più. Il server dei nomi, per esempio, "sa" anche quale computer accetta le e-mail per tutto il dominio; si tratta del cosiddetto *Mail exchanger (MX)*.

La configurazione dell'accesso al server dei nomi sotto SUSE LINUX viene descritta nel capitolo 14.6 a pagina 339.

whois

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.

14.2 IPv6 – l'Internet di prossima generazione

Come conseguenza del boom del *World Wide Web* , l'Internet, e con esso il numero dei computer che "parlano" 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 saprete, 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 "classe C" 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.

14.2.1 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 14.2.2 a pagina 321.

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 "Neighbor Discovery Protocol" (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 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 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 (vedi la sezione 14.2.3 a pagina 325). 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.e. SMB) devono inviare i propri pacchetti dati via broadcast agli host della rete locale, sotto IPv6 potete procedere in modo più differenziato. Tramite un multicast 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*).

14.2.2 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, meccanismi intelligenti preposti all'allocazione dell'indirizzo di rete e la possibilità del "multihoming" (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 agli appartenti del gruppo che in base al protocollo di routing sono quelli più vicini al mittente. Gli indirizzi anycast vengono utilizzati per consentire al terminale di rilevare il server richiesto all'interno della propria rete. Tutti i server 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 ....

Struttura di un indirizzo IPv6

L'indirizzo IPv6 è composto da otto blocchi di 16 bit ciascuno, separati dal carattere `:` (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 14.3 vi mostra questo procedimento con tre modi di rappresentare lo stesso indirizzo.

Exempio 14.3: *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 14.4 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.

Exempio 14.4: *Indirizzo IPv6 con prefisso*

```
fe80::10:1000:1a4/64
```

IPv6 ha diversi prefissi che hanno un significato ben preciso (vedi la tabella 14.4 nella pagina successiva).

Tabella 14.4: *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.e. 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 i seguenti spazi 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.e. `10.x.x.x`).
`ff`	Indirizzi IPv6 *multicast* che iniziano con `ff` sono indirizzi multicast.

Gli indirizzi unicast si compongono di tre parti:

Public Topology La prima parte, che include tra l'altro uno dei prefissi sopramenzionati, 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 basilare 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 (vedi la sezione 14.2.3 a fronte). Gli host IPv4/IPv6 possono in tal modo comunicare con gli host che si trovano in una rete prettamente IPv4.

Indirizzo IPv6 mappato IPv4 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 diversi 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 a livello mondiale. Solo le parti inerenti al "Site Topology" o "Public Topology" possono variare a seconda della rete a cui appartiene l'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.

14.2.3 IPv4 versus IPv6

Ce ne vorrà di tempo prima che tutti i computer 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 computer è resa possibile grazie al "dual stack". Resta comunque la questione del modo in cui computer IPv6 possano comunicare con computer IPv4, e del modo in cui realizzare il trasporto di IPv6 attraverso reti IPv4 che al momento sono quelle maggiormente diffuse. Tunneling ed indirizzi di compatibilità (vedi la sezione 14.2.2 a pagina 322) 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 estremità del tipo IPv4. Va indicato l'indirizzo meta IPv6 (oppure il relativo prefisso) dei pacchetti IPv6 "imballati", e l'indirizzo IPv4 remoto che riceverà i pacchetti trasmessi via 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 "imballati"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 la 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 reti 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'RFC3056.

IPv6 Tunnel Broker Qui dei server particolari creano i tunnel in modo automatico. L'RFC di riferimento è l' RFC3053.

Nota

L'iniziativa 6Bone

Su Internet già "di vecchio stampo" troviamo *6Bone* (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 a questo nuovo protocollo. Per ulteriori informazioni consultate il sito di 6Bone.

Nota

14.2.4 Ulteriore documentazione e link per IPv6

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).

14.3 Configurazione manuale della rete

La configurazione manuale della rete dovrebbe sempre essere la seconda scelta. Noi consigliamo di usare YaST. E' fondamentale che tutte le interfacce di rete vengano avviate con lo script `/sbin/ifup`. Per fermare o controllare un interfaccia vi è `ifdown` e `ifstatus`.

Se siete in possesso solo di una scheda di rete integrata, basta configurare le interfacce tramite i loro nomi. Con `ifup eth0`, `ifstatus eth0` e `ifdown eth0` avviate, controllate e fermate l'interfaccia di rete `eth0`. I file di configurazione utilizzati si trovano sotto `/etc/sysconfig/network/ifcfg-eth0`. `eth0` è in questo caso contemporaneamente il nome dell'interfaccia e il nome per la configurazione della rete.

La configurazione della rete può vertere anche sull'indirizzo hardware (indirizzo MAC) di una schede di rete. Per realizzare ciò, si usa un file di configurazione `ifcfg-<indirizzohardwaresenzaiduepunti>`. L'indirizzo hardware va scritto minuscolo, così come emesso da `ip link`;

(`ifconfig` utilizza le maiuscole). Se `ifup` trova un file di configurazione adatto all'indirizzo hardware, viene ignorato possibilmente anche un `ifcfg-eth0` esistente.

Con schede di rete hotplug, il tutto è un pò più complesso. Se siete in possesso di una scheda del genere, continuate con la sezione 14.3.1.

Visto che nel caso di schede di rete hotplug, la correlazione tra nome dell'interfaccia e la scheda è un fatto in prima linea "casuale", la configurazione di una tale scheda non viene archiviata con il nome dell'interfaccia, ma con il nome che descrive il tipo di hardware utilizzato e il punto di connessione, di seguito denonimato descrizione dell'hardware. `ifup` in questo caso va richiamato con due argomenti, la precisa descrizione dell'hardware e l'attuale nome dell'interfaccia. Successivamente `ifup` rivela la configurazione che si adatta il più possibile alla descrizione hardware.

Prendiamo come esempio un portatile con due slot PCMCIA e una scheda di rete Ethernet PCMCIA. Inoltre questo dispositivo contiene una scheda di rete integrata con il nome di interfaccia `eth0`. Se questa scheda è inserita nello slot `0`, la descrizione dell'hardware sarà `eth-pcmcia-0`. cardmgr o lo script di rete hotplug inizializzano `ifup eth-pcmcia-0 eth1`. Ora `ifup` cerca di stabilire se sotto `/etc/sysconfig/network/` vi sia un file `ifcfg-eth-pcmcia-0`. In caso negativo continua a cercare `ifcfg-eth-pcmcia`, `ifcfg-pcmcia-0`, `ifcfg-pcmcia`, `ifcfg-eth1` e `ifcfg-eth`. Il primo che trova viene utilizzato come file di configurazione. Se dunque va creata una configurazione di rete che deve valere per tutte le schede di rete PCMCIA (in tutti gli slot), essa deve chiamarsi `ifcfg-pcmcia`, la quale verrebbe usata per `eth-pcmcia-0` come anche per una scheda token-ring nello slot 1 `tr-pcmcia-1`.

Anche in questo caso la configurazione in base all'indirizzo hardware ha precedenza assoluta. Per motivi di chiarezza nell'esempio l'abbiamo omesso.

YaST configura schede hotplug per vie traverse. Alle varie configurazioni per questo tipo di scheda viene assegnato un numero. Perciò YaST scrive le impostazioni per schede PCMCIA sempre su `ifcfg-eth-pcmcia-<numeroprogressivo>`. Per fare in modo che la configurazione si applica a tutti gli slot, viene creato un link `ifcfg-eth-pcmcia` verso questo file. Questo va tenuto presente, se configurate in parte con ed in parte senza YaST.

14.3.1 File di configurazione

Questo paragrafo riassume i file di configurazione di rete e spiega la loro funzione ed il formato utilizzato.

/etc/sysconfig/network/ifcfg-*

Questi file contengono dati specifici per un'interfaccia di rete. Possono essere denominati secondo il nome dell'interfaccia (`ifcfg-eth2`), l'indirizzo hardware di una scheda di rete (`ifcfg-000086386be3`) o secondo la descrizione hardware per una scheda (`ifcfg-usb`). Se volete fare uso di alias di rete, i file corrispondenti sono semplicemente `ifcfg-eth2:1` o `ifcfg-usb:1`. Lo script `ifup` riceve all'occorrenza oltre al nome di interfaccia anche una precisa descrizione di hardware, per poi cercare i file che meglio si adattano alla configurazione.

I file contengono l'indirizzo IP (`BOOTPROTO=static`, `IPADDR=10.10.11.214`) o l'istruzione di utilizzare DHCP (`BOOTPROTO=`"dhcp"). L'indirizzo IP dovrebbe includere la maschera di rete (`IPADDR=`"10.10.11.214/16"). La pagina di manuale relativa a `ifup` contiene l'elenco completo delle variabili. Inoltre, possono essere utilizzate tutte le variabili dai file `dhcp`, `wireless` e `config` nei file `ifcfg-*`, se una impostazione altrimenti generale debba essere valida solo per una interfaccia.

/etc/sysconfig/network/config,dhcp,wireless

Il file `config` contiene impostazioni generali per il comportamento di `ifup`, `ifdown` e `ifstatus`. Le possibilità sono ben commentate. Similmente vi sono dei commenti in `dhcp` e `wireless`, dove trovano spazio impostazioni generali per DHCP e schede di rete radio. Tutte le variabili di questi file possono essere utilizzate anche in `ifcfg-*`, e chiaramente hanno lì precedenza.

/etc/resolv.conf

Come già il file `/etc/host.conf`, anche questo file, influisce sulla risoluzione dei nomi dei computer tramite la libreria *resolver*.

Qui si indica a quale dominio appartenga l'host (parola chiave `search`) e quale sia l'indirizzo del server dei nomi (parola chiave `nameserver`) che deve venire indirizzato. Possono venire indicati più di un nome di dominio. Al momento della risoluzione di un nome non del tutto qualificato si cerca di creare un nome valido e completamente qualificato dalle registrazione in `search`. Diversi server dei nomi possono venir resi noti tramite più righe inizianti con `nameserver`. I commenti vengono introdotti da #.

Il file 14.5 nella pagina successiva mostra un esempio per `/etc/resolv.conf`.

Exempio 14.5: `/etc/resolv.conf`

```
# Il nostro dominio
search example.com
#
# Usiamo sole (192.168.0.20) come server dei nomi
nameserver 192.168.0.20
```

YaST immette qui il server dei nomi (name server) indicato!

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 ordinatamente, anche se le modifiche sono state eseguite in ordine sparso. Cosa che può tranquillamente accadare, 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`

Con `modify_resolvconf check`, YaST può rilevare se `resolv.conf` sia stato modificato ed avvertire l'utente che tali modifiche andranno perse con il ripristino della versione originale. Alternativamente, YaST non si serve di `modify_resolvconf`: modifiche apportate al file resolv.conf tramite YaST ed una modifica manuale sono equivalente. In entrambi i casi, si tratta di una modifica mirata e duratura, mentre le modifiche dei servizi menzionati sono di natura puramente temporanea.

/etc/hosts

In questo file (vd. file 14.6 a fronte) 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 computer, in questo file viene annotata una riga consistente dell' indirizzo-IP, nome qualificato e nome dell'host (p.es. `terra`). L'indirizzo IP deve trovarsi all'inizio della riga, le registrazioni vengono separate da spazi o da tabulazioni. I commenti vengono preceduti da #.

Exempio 14.6: /etc/hosts

```
127.0.0.1 localhost
192.168.0.20 sole.example.com sole
192.168.0.0 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 (vedi file 14.7).

Exempio 14.7: /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, vedi le impostazioni in `/etc/nsswitch.conf`! Ogni parametro deve trovarsi in una propria riga, commenti vengono introdotti da #. La tabella 14.5 mostra i parametri possibili.

Tabella 14.5: *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 influenzano lo *spoofing* del server dei nomi, ma non influiscono sulla configurazione della rete.

trim `nome di dominio`	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.

Un esempio per `/etc/host.conf` mostra il file 14.8.

Exempio 14.8: *`/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) (vedi la pagina di manuale di `man 5 nsswitch.conf`, come pure per maggiori dettagli *The GNU C Library Reference Manual*, il capitolo "System Databases and Name Service Switch"; vd. il `libcinfo`).

Nel file `/etc/nsswitch.conf` viene stabilito in quale successione verranno richieste determinate informazioni. Un esempio per `nsswitch.conf` viene mostrato nel file 14.9. I commenti vengono introdotti da #. Lì per esempio, la registrazione nella banca dati `hosts` significa che una richiesta viene inviata a `/etc/hosts` (`files`) tramite DNS (cfr. sezione 14.6 a pagina 339)).

Exempio 14.9: */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 14.6; in futuro ci saranno anche `automount`, `bootparams`, `netmasks` e `publickey`.

Tabella 14.6: *Banche dati disponibili tramite /etc/nsswitch.conf*

`aliases`	Alias di mail, usato da `sendmail`; vedi la pagina di manuale `man 5 aliases`.
`ethers`	Indirizzi Ethernet.
`group`	Usato da `getgrent` per gruppi di utenti; vedi la pagina di manuale `man 5 group`.
`hosts`	Usato da `gethostbyname` e funzioni simili, per i nomi degli host e indirizzi IP.
`netgroup`	Elenco valido nella rete di host e utenti per regolare i diritti d'accesso; vedi la pagina di manuale `man 5 netgroup`.
`networks`	Nomi ed indirizzi di rete usati da `getnetent`
`passwd`	Password degli utenti usate da `getpwent`; vedi la pagina di manuale `man 5 passwd`.
`protocols`	Protocolli di rete usati da `getprotoent`; vedi 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`; vedi la pagina di manuale `man 5 shadow`.

Le possibilità di configurazione delle banche dati NSS, vengono illustrate nella tabella 14.7.

Tabella 14.7: *Possibilità di configurazione delle banche dati NSS*

`files`	Accesso diretto ai file, per esempio su `/etc/aliases`.
`db`	Accesso tramite una banca dati.
`nis`	Vedi la sezione 14.8 a pagina 367.
`nisplus`	

`dns`	Da usare come estensione solo con `hosts` e `networks`.
`compat`	Da usare come estensione solo con `passwd`, `shadow` e `group`

Inoltre con determinati risultati di ricerca è possibile provocare reazioni differenti; i dettagli a riguardo si trovano nella pagina di manuale

/etc/nscd.conf

Tramite questo file viene configurato l'nscd (*Name Service Cache Daemon*); vedi `man 8 nscd` e `man 5 nscd.conf`. Sono interessate le informazioni contenute in `passwd` e `groups`. `hosts` non viene memorizzato temporaneamente (chaching), dato che il sistema non puó piú fare affidamento su "forward/reverse lookups" di questo servizio di nome.

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: `rcnscd restart`

/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 con il nome dell'host!

14.3.2 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*, (vd. tabella 14.8).

Tabella 14.8: *Alcuni script di inizializzazione dei programmi di rete*

`/etc/init.d/network`	Questo script si occupa della configurazione dell'hardware e del software di rete durante la fase di avvio del sistema.

`/etc/init.d/inetd`	Lancia l'xinetd a cui si può ricorrere per mettere a disposizione all'occorenza dei servizi di sistema sul sistema; ad es. può lanciare vsftpd non appena venga inizializzata una connessione FTP.
`/etc/init.d/portmap`	Lancia il port mapper che è necessario per poter usare i server RPC, come per esempio un server NFS.
`/etc/init.d/nfsserver`	Inizializza il server NFS.
`/etc/init.d/postfixl`	Controlla il processo postfix.
`/etc/init.d/ypserv`	Lancia il server NIS.
`/etc/init.d/ypbind`	Lancia il client NIS.

14.4 L'integrazione nella rete

Oggi si può tranquillamente asserire che TCP/IP è diventato il protocollo di rete standard di cui si servono tutti i recenti sistemi operativi per realizzare la comunicazione via rete. Comunque, Linux supporta anche altri protocolli di rete come, ad es., IPX, usato (in passato) da Novel Netware o anche Appletalk utilizzato dai computer Macintosh. In questo ambito, parleremo solo dell'integrazione di un computer Linux in una rete TCP/IP. Se volete integrare schede di rete "esotiche" come Arcnet, Token-Ring o FDDI, trovate ulteriori informazioni nei sorgenti del kernel `/usr/src/linux/Documentation`, che installerete con il pacchetto `kernel-source`.

14.4.1 Premesse

Il computer 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 `ifstatus eth0` che indica il dispositivo di rete `eth0`.

Il driver per la scheda di rete di solito è un modulo del kernel (soprattutto per quanto riguarda il kernel di SUSE), per questo motivo bisogna registrare come 'alias' il nome del modulo in `/etc/modules.conf`. Per la prima

scheda Ethernet p.es. in questo modo: `alias eth0 tulip`. Ciò avviene automaticamente, se in linuxrc, durante la prima installazione, viene caricato il supporto driver per la scheda di rete. Successivamente, questo compito può venire svolto con YaST.

Con schede di rete hotplug (p.e. PCMCIA o USB) i driver vengono rilevati automaticamente al momento del loro inserimento; non bisogna configurare alcunché.

14.4.2 Configurazione con YaST

La scheda di rete si lascia configurare in modo veloce con YaST. Selezionate nel Centro di controllo di YaST la voce 'Rete/Basilare' ed infine 'Configurazione della scheda di rete'. In questo dialogo integrate una scheda di rete con 'Aggiungi', con 'Elimina' la scheda viene rimossa dalla configurazione e con 'Modifica' potete modificare le impostazioni della scheda di rete.

Attivate il punto 'Hardware', per modificare, con 'Modifica', i dati dell'hardware di una scheda rete già configurata: ora arrivate al menu della configurazione dei dati dell'hardware della vostra scheda rete. Il menu è rappresentato nella figura 14.3 a fronte.

Normalmente, YaST configura già durante l'installazione il driver per la vostra scheda di rete e attiva la scheda di rete stessa: per questa ragione, le impostazioni manuali dei parametri dell'hardware sono necessarie solo se usate più di una scheda di rete o se l'hardware di rete non viene riconosciuto automaticamente. In questo caso, selezionate il punto 'Aggiungi' affinchè possa venir scelto un nuovo modulo del driver.

In questo dialogo, potete impostare il tipo della scheda di rete e, nel caso di schede ISA, l'interrupt da usare e l'indirizzo IO. Ad alcuni driver di rete potete passare anche speciali parametri come p.e. l'interfaccia da usare, o se p.e. volete utilizzare sulla scheda il connettore `RJ-45` o `BNC`. Consultate a proposito la documentazione del modulo driver; per PCMCIA e USB basta attivare la relativa casella.

Dopo aver inserito i parametri dell'hardware potete configurare gli altri dati relativi all'interfaccia della rete. Per attivare la scheda di rete appena configurata ed assegnarle un indirizzo IP, selezionate il punto 'Interfaccia' nel dialogo 'Configurazione di base della rete'. Selezionate il numero della scheda e cliccate quindi su 'Modifica': apparirà un nuovo dialogo, nel quale potrete scegliere l'indirizzo IP e gli altri dati della rete IP. Se allestite una vostra rete, potete orientarvi, per l'attribuzione degli indirizzi, al paragrafo 14.1 a pagina 310 o alla tabella 14.3 a pagina 317. Altrimenti, immettete nei campi previsti, gli indirizzi assegnati dal vostro amministratore di rete.

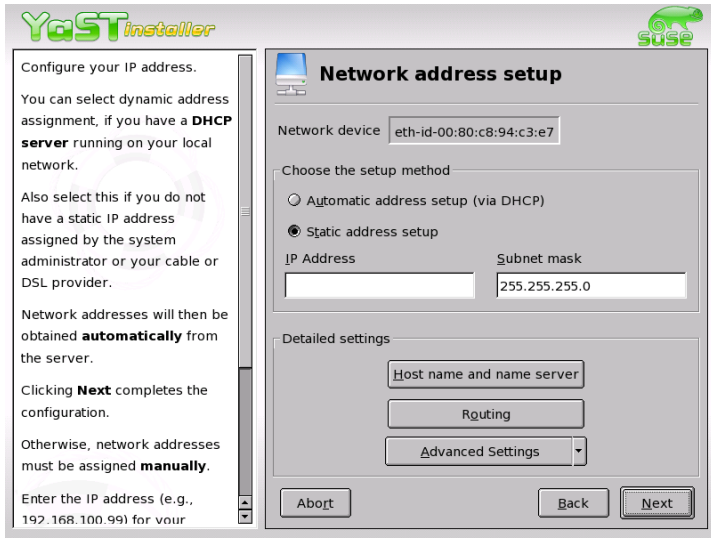

Figura 14.3: *Configurazione dei parametri dell'hardware*

Affinché la risoluzione dei nomi funzioni come descritto nella sezione 14.6 a pagina 339, non dimenticate di impostare un server dei nomi sotto 'Nome host e DNS'. Tramite la voce 'Routing' potete impostare il routing. Per eseguire impostazioni avanzate, selezionate il punto 'Configurazione per esperti'.

Se utilizzate schede di rete radio, attivate la casella 'Wireless Device'. Le principali impostazioni si possono eseguire in un dialogo a parte. Si tratta in particolare del modo di funzionamento, nome della rete e una chiave per la trasmissione dei dati cifrata.

La configurazione della rete è a questo punto conclusa. YaST lancia SuSEconfig ed immette le vostre indicazioni nei relativi file. Affinché le impostazioni vengono applicate, dovete riconfigurare i programmi interessati, e riavviare i rispettivi demoni immettendo: `rcnetwork restart` come utente `root`.

14.4.3 Hotplug/PCMCIA

Un caso particolare è rappresentato da schede di rete hotplug, come dispositivi PCMCIA o USB. Al contrario di schede di rete integrate che hanno un

nome di dispositivo fisso, p.es. `eth0`, queste schede ottengono all'occorrenza, in modo dinamico, un nome di dispositivo ancora libero. Per evitare dei conflitti con schede di rete integrate, PCMCIA e l'hotplug vengono inizializzati durante il boot dopo che si stata inizializzata la rete.

Queste schede vengono configurate automaticamente non appena vengono inserite o rilevate al boot. Perciò non è necessario avviare PCMCIA prima della rete. Se questa scheda fosse amministrata solo dallo script di avvio delle rete durante il boot, non vi sarebbe più la possibilità di sostituirla mentre il sistema è in esecuzione.

14.4.4 Configurare IPv6

Se volete impostare IPv6, normalmente, non dovete effettuare alcuna configurazione sulle postazioni di lavoro. È però necessario caricare il supporto per IPv6; potete farlo eseguendo il comando `modprobe ipv6` come `root`.

Grazie alla filosofia della configurazione automatica di IPv6, viene attribuito alla scheda di rete, 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 dal `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 configurazione di routing.

Per poter assegnare comodamente un indirizzo IPv6 ad una postazione di lavoro, è consigliabile installare e configurare un router con il programma radvd oppure zebra. In questo modo, alle postazioni di lavoro viene assegnato automaticamente un indirizzo IPv6.

Per configurare diversi tunnel ricorrendo ai file sotto `/etc/sysconfig/network` consultate la pagina di manuale di ifup (`man ifup`).

14.5 Il routing con SUSE LINUX

A partire da SUSE LINUX 8.0, la tabella di routing si imposta nei file di configurazione `/etc/sysconfig/network/routes` e `/etc/sysconfig/network/ifroute-*`.

Nel file `/etc/sysconfig/network/routes` possono venire registrate tutte le route statiche che sono necessarie per i diversi compiti di un sistema: route ad un computer, route ad un computer tramite un gateway e route ad una rete. Ecco ad esempio come configurare il gateway di default per route statiche:

```
default GATEWAY - -
```

laddove GATEWAY è l'indirizzo IP del gateway.

Per tutte le interfacce che necessitano un routing particolare, si può definire un file proprio per ogni interfaccia: `/etc/sysconfig/network/ifroute-*`. Al posto di `*` inserite il nome dell'interfaccia. Le registrazioni possono assumere il seguente aspetto:

```
DESTINATION           GATEWAY NETMASK   INTERFACE [ TYPE ] [ OPTIONS ]
DESTINATION           GATEWAY PREFIXLEN INTERFACE [ TYPE ] [ OPTIONS ]
DESTINATION/PREFIXLEN GATEWAY -         INTERFACE [ TYPE ] [ OPTIONS ]
```

Se GATEWAY, NETMASK, PREFIXLEN o INTERFACE non vengono indicati, al loro posto va inserito un `-`. Le registrazioni TYPE e OPTIONS possono anche essere omesse.

- Nella prima colonna si indica la meta di una route: può trattarsi di un l'indirizzo IP di una rete o host o, nel caso di server dei nomi *raggiungibili*, anche del nome completo, qualificato della rete o host.
- La seconda colonna contiene o il gateway di default o un gateway dietro cui è raggiungibile un host o una rete.
- La terza colonna contiene la maschera di rete per reti o host dietro un gateway. Per host dietro un gateway, la maschera è ad es. `255.255.255.255`
- L'ultima colonna è importante solo per le reti collegate al computer locale (loopback, ethernet, ISDN, PPP, ...). Qui si deve specificare il nome del dispositivo.

14.6 DNS: Domain Name System

Compito del DNS *Domain Name System* è di risolvere i nomi di dominio e host in indirizzi IP. Prima di configurare un proprio server dei nomi, leggete le informazioni generali riguardanti il DNS che trovate nella sezione 14.1.3 a pagina 317.

I seguenti esempi di configurazione si riferiscono a BIND 9, che adesso rappresenta lo standard in SUSE LINUX.

14.6.1 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 corretta risoluzione dei nomi, senza 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 va bene, 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 si trova sotto `/usr/share/doc/packages/bind9/sample-config`.

Non si dovrebbe impostare un dominio ufficiale, finché l'istituzione competente – per '.it' si tratta dell' ITNIC non ve ne assengni 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` sulla riga 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 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:

```
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 14.10 sono stati scelti a caso, dovrete adattarli in base ai vostri dati effettivi.

Exempio 14.10: *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 `.` di `type hint` che dovrebbero essere comunque presenti. 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`.

14.6.2 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`. Ma questo sarà trattato 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 14.11 vi mostra un esempio di un `/etc/named.conf` ridotto all'osso.

Exempio 14.11: *File minimale /etc/named.conf*

```
options {
        directory "/var/lib/named";
        forwarders { 10.0.0.1; };
        notify no;
};

zone "localhost" in {
        type master;
        file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
        type master;
        file "127.0.0.zone";
};

zone "." in {
        type hint;
        file "root.hint";
};
```

14.6.3 Le opzioni di configurazione principali della sezione options

directory "/var/lib/named"; indica la directory in cui BIND trova i file con i dati delle zone.

forwarders 10.0.0.1; ; 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.

forward first; fa in modo che le richieste DNS vengano inoltrate "forwarded", prima di 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; 192.168.0.1; ;
comunica a BIND, su quali interfacce di rete e su quale porta è in ascolto per eventuali richieste dei client. L'indicazione `port 53` può venire omessa, poiché 53 è la porta standard. Omettendo completamente questa registrazione, vengono usate come standard tutte le interfacce.

listen-on-v6 port 53 any; ; indica a BIND su quale porta è in ascolto per richieste 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; questa registrazione deve essere utilizzata per richieste tramite IPv6.

allow-query 127.0.0.1; 192.168.1/24; ;
definisce le reti da cui i client possono inviare delle richieste DNS. `/24` è un'abbreviazione per la maschera di rete, in questo caso `255.255.255.0`.

allow-transfer ! *; ; regola quali computer 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.

14.6.4 La sezione di configurazione logging

BIND permette di configurare in modo flessibile l'attività di logging. Normalmente, le preimpostazioni dovrebbero rilevarsi sufficienti. L'esempio 14.12 vi mostra la variante più semplice di una tale registrazione, e sopprime completamente il logging:

Exempio 14.12: *Il logging viene soppresso*

```
logging {
        category default { null; };
};
```

14.6.5 Struttura delle registrazioni delle zone

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.file 14.13.

Exempio 14.13: *L'indicazione zone per mio-dominio.it*

```
zone "mio-dominio.it" in {
       type master;
       file "mio-dominio.zone";
       notify no;
};
```

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, però, anche essere uno "slave"); cfr. esempio 14.14 nella pagina successiva.

Exempio 14.14: *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 10.0.0.1;; 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.

14.6.6 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.

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 due volte. La mancanza di questo punto alla fine o la sua posizione errata sono sicuramente gli errori più comuni nella configurazione di server dei nomi.

Osserviamo ora il file zona `mondo.zone` responsabile per il dominio Domain `mondo.all`; cfr. il file 14.15.

Exempio 14.15: *File /var/lib/named/mondo.zone*

```
1  $TTL 2D
2  mondo.all IN SOA      gateway  root.mondo.all.(
3                2003072441  ; serial
4                1D          ; refresh
5                2H          ; retry
6                1W          ; expiry
7                2D )        ; minimum
8
9                IN NS       gateway
10               IN MX       10 sole
11
12  gateway      IN A        192.168.0.1
13               IN A        192.168.1.1
14  sole         IN A        192.168.0.2
15  luna         IN A        192.168.0.3
16  terra        IN A        192.168.1.2
17  marte        IN A        192.168.1.3
18  www          IN CNAME    luna
```

Rigo 1: `$TTL` definisce il TTL standard, valido per l'intero contenuto di questo file: due giorni, in questo caso (2D = 2 days). TTL significa Time to Live, ovvero 'scadenza'.

Rigo 2: Ha inizio qui il `SOA control record`:

- 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 di 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 un'ennesima 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 debbano restare nella cache che non è stato possibile risolvere.

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 il 'reverse lookup' (la risoluzione inversa) 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`.

Exemplo 14.16: *Risoluzione inversa dell'indirizzo*

```
1  $TTL 2D
2  1.168.192.in-addr.arpa. IN SOA gateway.mondo.all. root.mondo.all. (
3                           2003072441     ; serial
4                           1D              ; refresh
5                           2H              ; retry
6                           1W              ; expiry
7                           2D )            ; minimum
8
9                           IN NS           gateway.mondo.all.
10
11 1                     IN PTR          gateway.mondo.all.
12 2                     IN PTR          terra.mondo.all.
13 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: vd. 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.

14.6.7 Transazioni sicure

Grazie alle "Transaction SIGnatures" (TSIG) si realizza una transazione sicura. Vengono utilizzate delle chiavi di transazione (*transaction keys*) e firme di transazione (*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 vedi la pagina di manuale `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.e. `ejIkuCyyGJwwuN3xAteKgg==`). In seguito `Khost1-host2.+157+34265.key` dovrebbe venir copiato in modo sicuro (p.e. con `scp`) su host remoti e lì essere inserito in `/etc/named.conf` per realizzare una comunicazione sicura tra `host1` e `host2`:

```
key host1-host2. {
  algorithm hmac-md5;
  secret "ejIkuCyyGJwwuN3xAteKgg=="
};
```

Attenzione

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 deporre la chiave in un file protetto ed includerlo di seguito.

Attenzione

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`.

14.6.8 Aggiornamento dinamico dei dati di zona

Con aggiornamento dinamico (*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 vedi la pagina di manuale di `nsupdate`. L'aggiornamento deve avvenire assolutamente, per motivi di sicurezza, tramite transazioni sicure (TSIG); cfr. la sezione 14.6.7 a pagina 349.

14.6.9 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.

14.6.10 Ulteriori informazioni

Rimandiamo al *BIND Administrator Reference Manual* che trovate sotto `/usr/share/doc/packages/bind9/`, nonché agli RFC ivi menzionati e le pagine di manuale di BIND 9.

14.7 LDAP — Un servizio directory

In ambienti di lavoro collegati in rete è determinante che le informazioni importanti siano tenute in serbo in modo strutturato e che siano ritrovabili immediatamente. Un caos di dati non incombe solo sugli utenti di Internet, anche la ricerca di dati importanti all'interno di una rete aziendale può diventare un'impresa disperata: dove trovo il numero del mio collega XY? Qual'è il suo indirizzo e-mail?

Questo problema viene risolto da un servizio directory il quale alla stregua delle pagine gialle (ingl.*Yellow Pages*), che tutti conosciamo dalla vita quotidiana, 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 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 al fine di essere accessibile e consultabile in modo semplice e veloce:

- 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, la lista dei numeri di telefono 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. 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 *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 'alleggerito' di alcune funzionalità di DAP, può essere utilizzato cross-plattform e fa un uso parsimonioso delle risorse, senza dover rinunciare alla disposizione gerarchia 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 previsto all'inizio. Con slapd esiste un server open source con il quale archiviare i dati 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 i dati 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

14.7.1 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 di `group/`, `hosts/`, `mail/`, `netgroup/`, `networks/`, `passwd/`, `printcap/`, `protocols/`, `rpc/` e `services/` contenuti nei file e nelle directory di `/etc/` . 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 qualisiasi 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.

14.7.2 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.

Foglia 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` (*country*), `dc` (*domainComponent*) oppure `o`(*organization*).

Le relazioni che intercorrono all'interno di un albero di directory LDAP vengono illustrate nel seguente esempio (vedi figura 14.4).

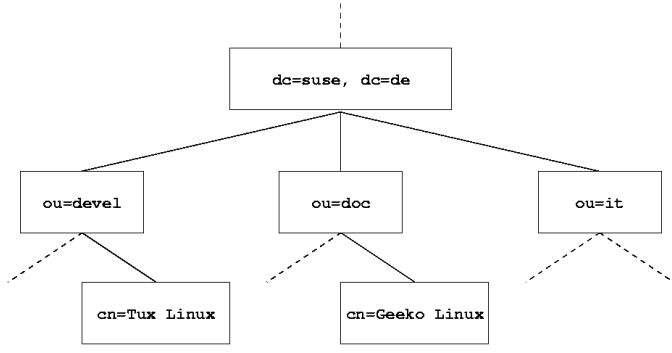

Figura 14.4: *Struttura di una directory LDAP*

L'intera figura comprende un *Directory Information Tree* esempio. Le registrazioni (*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 di oggetto*. La classe di oggetto 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 (vedi 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 14.9 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 14.9: *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* (Unita di organizzazione)	doc	ou
inetOrgPerson	*inetOrgPerson* (Dati di persone per Intranet/Internet)	Geeko Linux	sn e cn

Nell'output 14.17 vedete un'estratto di una direttiva schema con commenti che vi aiuteranno a comprendere la sintassi di nuovi schemi.

Exempio 14.17: *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`.

14.7.3 Configurazione server con slapd.conf

`/etc/openldap/slapd.conf` è il file di configurazione del vostro server LDAP. 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.

Direttive globali in slapd.conf

Exempio 14.18: *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 (vedi l'output 14.18). 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 `rfc2307bis.schema`. Per ulteriori informazioni su questa problematica, consultate la documentazione OpenLDAP fornita a corredo.

Exempio 14.19: *slapd.conf: pidfile ed argsfile*

```
pidfile         /var/run/slapd.pid
argsfile /var/run/slapd.args
```

Questi due file contengono il PID (ingl.*process id*) e alcuni argomenti con i quali lanciare il processo slapd. Qui non è necessario apportare delle modifiche.

Exempio 14.20: *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 14.20 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 che vi aiutano a comprendere tale processo.

- 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 seguenti registrazioni.

- ⟨*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 (vedi la tabella 14.10):

Tabella 14.10: *Gruppi utenti con permesso di accesso*

Identificatore	Significato
*	Tutti gli utenti senza eccezione alcuna
`anonymous`	Utenti non autenticati("anonimi")
`users`	Utenti autenticati
`self`	Utenti in relazione con l'oggetto meta
`dn=<regex>`	Tutti gli utenti per cui vale questa espressione regolare

- ⟨*access*⟩ specifica il tipo di accesso. Si distingue tra le possibilità riportate nella tabella 14.11

Tabella 14.11: *Tipi di accesso*

Identificatore	Significato
`none`	Accesso negato
`auth`	per la presa di contatto con 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'output 14.21 vedete un esempio per un controllo degli accessi semplice su cui potete intervenire a piacimento tramite l'uso di espressioni regolari.

Exempio 14.21: *slapd.conf: esempio per il controllo degli accessi*

```
access to  dn.regex="ou=([^,]+),dc=suse,dc=de"
by cn=administrator,ou=$1,dc=suse,dc=de write
by user read
by * none
```

Questa regola stabilisce che solo il relativo 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.

Nota

impostare le regole di accesso

L'accesso viene negato se non vi è alcuna regola `access to` oppure alcuna direttiva `by <who>` 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.

Nota

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 nello stato 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`.

Direttive in slapd.conf riguardanti la banca dati

Exempio 14.22: *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 (vedi output 14.22) viene stabilito il tipo di banca dati, nell'esempio 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 per 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.

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 (vedi la sezione 14.7.4), 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 (vedi anche la sezione 13.5 a pagina 301) oppure create i relativi riferimenti dei script di avvio e di arresto sulla riga di comando tramite `insserv` (vedi la sezione 13.4.1 a pagina 299).

14.7.4 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.

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 *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 14.4 a pagina 355) assumerebbe il seguente aspetto (vedi l'esempio 14.23):

Exempio 14.23: *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
```

Nota

Codifica dei file LDIF

LDAP utilizza UTF-8 (Unicode). Gli accenti vanno quindi codificati correttamente. Utilizzate un editor che supporta UTF-8 (Kate) oppure una delle versioni più recenti di Emacs. Altrimenti dovreste rinunciare ai caratteri accentuati o utilizzare recode per ricodificare in UTF-8 le vostre immissioni.

Nota

Salvate il file sotto `<file>.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 file. Nell'esempio 14.24 nella pagina seguente vedete in dettaglio il comando `ldapadd`.

Exempio 14.24: *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` (vedi l'esempio 14.25) aggiungiamo l'addetto `Tux` alla nuova directory LDAP:

Exempio 14.25: *File LDIF per Tux*

```
# L'addetto Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
objectClass: inetOrgPerson
cn: Tux Linux
givenName: Tux
mail: tux@suse.it
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 relativamente di frequente i vostri dati, si consiglia di suddividerli in tanti oggetti, in modo da risparmiarvi la ricerca laboriosa degli oggetti da modificare in file grossi.

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 14.26.

Exempio 14.26: *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:

- Lanciate `ldapmodify` ed immettete la vostra password:

  ```
  ldapmodify -x -D cn=admin,dc=suse,dc=de -W

  Enter LDAP password:
  ```

- 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` per avere delle informazioni dettagliate su `ldapmodify` e la sua sintassi.

Come cercare e leggere dei dati della directory LDAP

OpenLDAP offre con `ldapsearch` un tool per la 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.e. 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 vostra 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 (`man ldapsearch`).

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
```

14.7.5 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 2.1 Administrator's Guide* (per i link vedi 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/admin21/quickstart.html` o a sistema installato reperibile sotto `/usr/share/doc/packages/openldap2/admin-guide/quickstart.html`

OpenLDAP 2.1 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/admin21/` o a sistema installato sotto `/usr/share/doc/packages/openldap2/admin-guide/index.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.

14.8 NIS: Network Information Service

Non appena sono diversi sistemi Unix a voler accedere a risorse condivise sulla rete, si dovrà 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 ed NFS. L'NFS serve alla dislocazione di file system nella rete e viene descritto più dettagliatamente nel paragrafo 14.9 a pagina 371.

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 ben altri fini (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.

14.8.1 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, alla 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 YaST vi chiederà di inserire il relativo CD o il DVD per poter eseguire l'installazione dei rispettivi pacchetti. Nella prima maschera di configurazione (Fig. 14.5 a fronte) 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 da 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 check box '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 ad un dialogo (Fig. 14.6 a pagina 370), in cui si può modificare la directory sorgente del server NIS

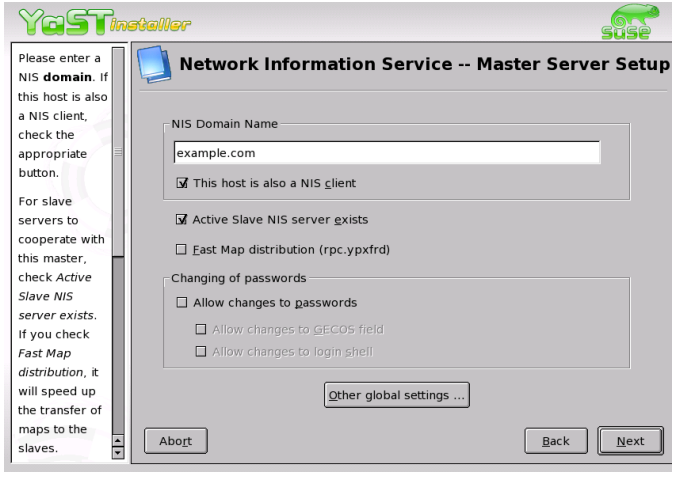

Figura 14.5: *YaST: tool di configurazione per server NIS*

(di default `/etc/`). Inoltre qui si possono raggruppare password e 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 è fate clic su 'Prossimo'. Se nella vostra rete non vi è nessun server slave giungete direttamente al seguente dialogo 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 intedete modificarle, fatelo solo con cognizione di causa.

Con 'Prossimo' arrivate all'ultimo dialogo, dove potete stabilire da quali reti possono provenire richieste per il server NIS (vd. Fig. 14.7 a pagina 371). Di solito si tratterà della vostra rete aziendale, in questo caso dovrebbero esserci le registrazioni

```
255.0.0.0       127.0.0.0
0.0.0.0         0.0.0.0
```

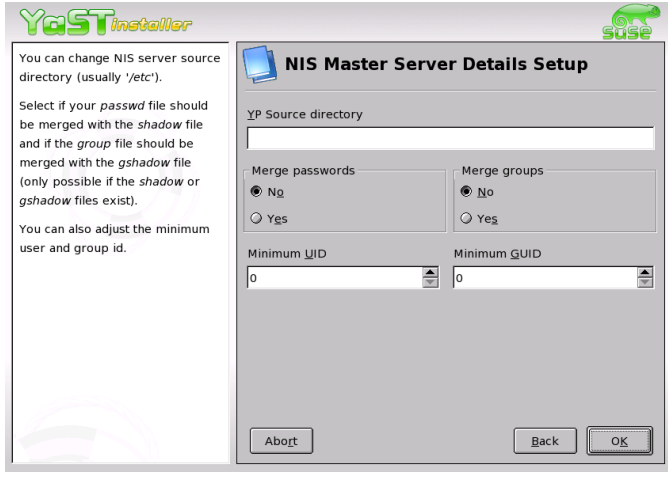

Figura 14.6: *YaST: server NIS: modificare directory e sincronizzare file*

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.

14.8.2 Il modulo client NIS in YaST

Questo modulo vi permette di configurare facilmente il client NIS. Dopo che nel dialogo iniziale avete indicato che intendete utilizzare NIS ed eventualmente l'automounter giungete al prossimo dialogo. 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 sezione 14.10 a pagina 377. Se il client dispone di un indirizzo IP fisso, dovete immettere manualmente il dominio e server NIS (vd. Fig. 14.8 a pagina 372). Tramite il bottone '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.

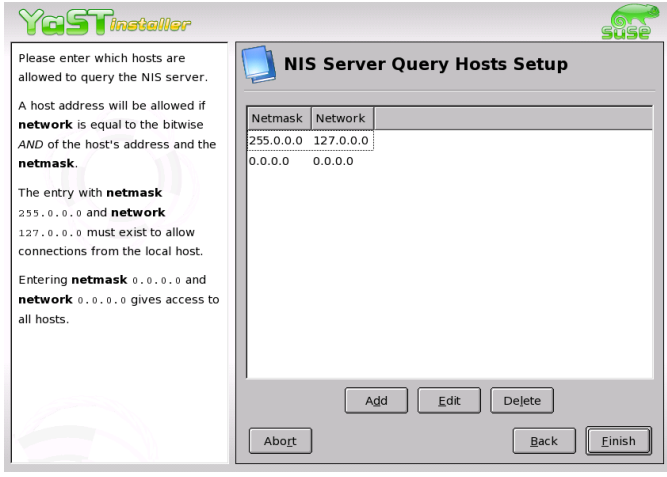

Figura 14.7: *YaST: server NIS: gli host con permesso di inviare richieste al server*

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`.

14.9 NFS – file system dislocati

Come abbiamo già accennato nel paragrafo 14.8 a pagina 367, l'NFS e l'NIS servono a rendere trasparente la rete all'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 collocare file system nella rete ("esportare"), e montare file system di altri computer ("importare"). Normalmente, tuttavia, si usano a questo scopo dei server con dischi capienti, i cui file system vengono poi montati dai client.

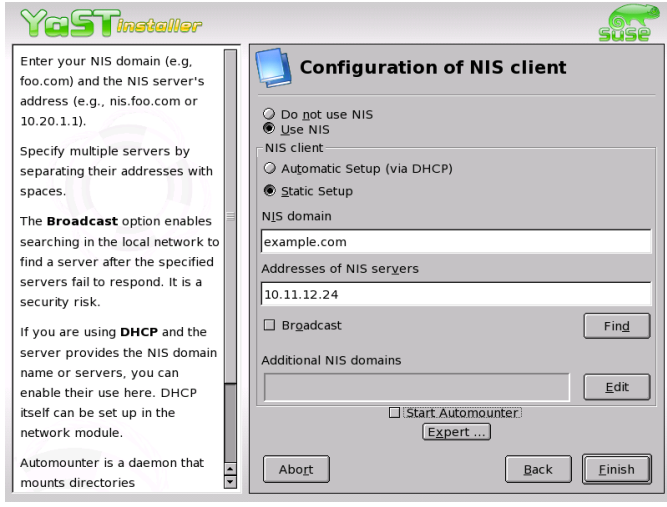

Figura 14.8: *Indicazione del dominio e dell'indirizzo del server NIS*

14.9.1 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 YaST. 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 (vd. Fig. 14.9).

14.9.2 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 `rcportmap> start` 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
```

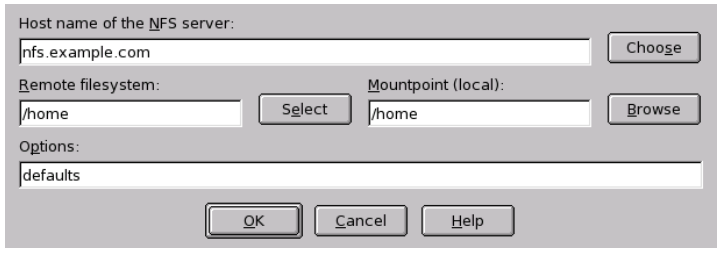

Figura 14.9: *Configurare il client NFS*

Per importare, ad esempio, le directory degli utenti dall'host sole, usate il comando:

```
mount sole:/home /home
```

14.9.3 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 directory e 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' e lì 'Server NFS'. (Fig. 14.10 nella pagina successiva).

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 (Fig. 14.11 a pagina 375). Per ogni host possono essere settate quattro opzioni, `host singolo`, `gruppi di rete`, `wildcard` e `reti IP`. Una descrizione dettagliata di queste opzioni si trova nelle pagine di manuale di `exports`.

Con 'Fine' concludete la configurazione.

14.9.4 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:

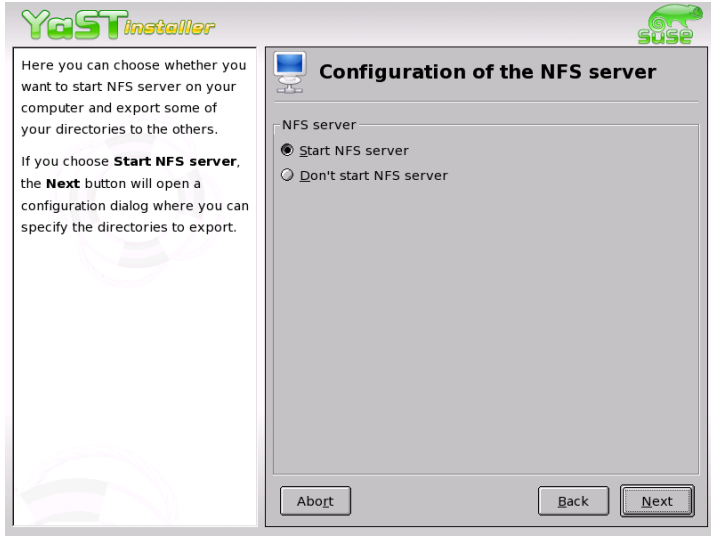

Figura 14.10: *Tool di configurazione per server NFS*

- 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`.

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).

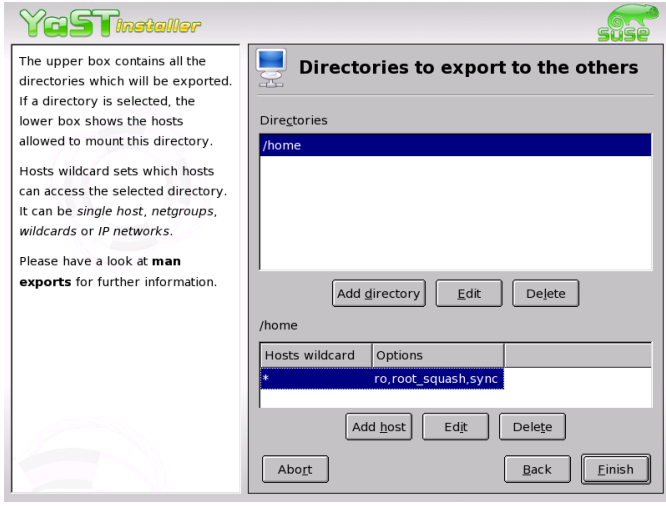

Figura 14.11: *Server NFS: immettere directory da esportare e host*

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 14.12: *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` vengono eseguiti con l' user-ID `65534 (-2)`, 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 `../`. È 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 file `exports` potrebbe, ad esempio, essere simile al file 14.27.

Exempio 14.27: */etc/exports*

```
#
# /etc/exports
#
/home            sole(rw)   venus(rw)
/usr/X11         sole(ro)   venus(ro)
/usr/lib/texmf   sole(ro)   venus(rw)
/                terra(ro,root_squash)
/home/ftp        (ro)
# End of exports
```

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 di digitare il comando:

```
rcnfsserver restart
```

14.10 DHCP

14.10.1 Il protocollo 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, li può munire costantemente delle stesse impostazioni, come pure assegnare 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 computer 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 adeguati.

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.e. un time server da cui richiedere l’ora attuale o un server di stampa. In quel che segue, vi forniremo una breve descrizione di DHCP. Prendendo spunto dall’esempio riportato di seguito intendiamo mostrare quanto sia semplice configurare centralmente anche la vostra rete tramite un server DHCP.

14.10.2 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 computer per rilevare il server DHCP. Se la cava senza un file di configurazione e normalmente dovrebbe funzionare anche senza doverlo configurare.

Per scenari più complessi, si può ricorrere al dhclient dell'ISC che potete amministrare tramite il file di configurazione `/etc/dhclient.conf`.

14.10.3 Il server DHCP dhcpd

Il *Dynamic Host Configuration Protocol Daemon* è il cuore di ogni sistema DHCP. Egli 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`:

Exempio 14.28: *Il file di configurazione /etc/dhcpd.conf*

```
default-lease-time 600;         # 10 minutes
max-lease-time 7200;            # 2  hours

option domain-name "cosmos.all";
option domain-name-servers 192.168.1.1, 192.168.1.2;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option subnet-mask 255.255.255.0;

subnet 192.168.1.0 netmask 255.255.255.0
 {
  range 192.168.1.10 192.168.1.20;
  range 192.168.1.100 192.168.1.200;
 }
```

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 dato 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 vedi sezione 14.6 a pagina 339.
- `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, viene definita un'altra rete con la maschera della sottorete. Infine, va stabilita un'area indirizzi dalla quale il demone DHCP possa attribuire indirizzi ai client richiedenti. 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 `rcdhcpdstart`, il demone DHCP che sarà subito a vostra disposizione.

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`.

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 passate con (Ctrl) + (Alt) + (F10)) alla console10.

14.10.4 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 sufficente 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 e solitamente unico al mondo formato da sei coppie di ottetti assegnato ad ogni dispositivo di rete, p.e. `00:00:45:12:EE:F4`.

Se al file di configurazione del file 14.28 a pagina 378 viene aggiunta una registrazione come nel file 14.29, il DHCPD fornirà in ogni caso gli stessi dati al computer corrispondente.

Exempio 14.29: *Aggiunte al file di configurazione*

```
host terra {
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 computer da definire (`host <hostname>`), 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 computer (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 terra.

Oggigiorno, come tipo di hardware viene generalmente usato `ethernet`, ma viene anche supportato `token-ring`, usato per la maggior parte nei sistemi IBM.

14.10.5 Particolarità di SUSE Linux

Per ragioni di sicurezza la versione SUSE del server ISC DHCP contiene la patch 'non-root/chroot' di Ari Edelkind che permette a dhcpd

- di girare come utente 'nobody'
- di girare in un ambiente chroot (`/var/lib/dhcp/`)

Il file di configurazione `/etc/dhcpd.conf` deve trovarsi in `/var/lib/dhcp/etc/`; lo script di inizializzazione lo copia in tale directory automaticamente all'avvio.

Questa funzionalità si lascia gestire tramite il 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 nell'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 `"-a /var/lib/dhcp/dev/log"` alla variabile `SYSLOGD_PARAMS` in `/etc/sysconfig/syslog` .

14.10.6 Ulteriori fonti di informazione

Se siete interessati ad informazioni dettagliate, visitate p.es. il sito dell'*Internet Software Consortium* (`http://www.isc.org/products/DHCP/`.

Dove troverete anche la documentazione relativa alla versione 3 del protocollo che al momento si trova in fase di beta testing. Naturalmente potrete consultare anche le pagine di manuale e in particolar modo `man dhcpd`, `man dhcpd.conf`, `man dhcpd.leases` e `man dhcp-options`.

Sono stati editi una serie di manuali che si occupano delle possibilità offerte dal *Dynamic Host Name Configuration Protocol*.

Infine, dhcpd è in grado di offrire a client richiedenti un file definito nel file di configurazione con il parametro *filename* che contiene un kernel avviabile. In questo modo è possibile avere dei client sprovvisti di un disco rigido che caricano sia il loro sistema operativo come pure i loro file eclusivamente via rete (*diskless clients*). La cosa può essere interessante sia da un punto di vista economico che da un punto di vista della sicurezza.

14.11 Sincronizzare l'orario con xntp

14.11.1 Introduzione

L'ora esatta svolge un ruolo di primo piano in tanti processi di sistema. A tal fine i computer hanno di solito un orologio integrato che spesso comun-

que si rivela di non essere all'altezza delle richieste avanzate da applicazioni come banca dati. Il modo per ovviare al problema consiste nel correggere continuamente l'orario del sistema locale oppure correggere l'orario tramite la rete. L'ora non dovrebbe venir spostata all'indietro ed i singoli passi nei quali viene spostata in avanti non dovrebbero superare un certo intervallo di tempo. É relativamente semplice correggere l'ora del sistema con ntpdate, però si ha un salto brusco dell'orario che non tutte le applicazioni riescono a tollerare.

Un approccio di sicuro interesse alla soluzione del problema viene offerto da xntp che permette di correggere l'ora di sistema locale continuamente in base a dei dati di correzione raccolti in precedenza, ricorrere a dei server dell'ora nella rete, oppure come terza possibilità consente di amministrare orari di riferimento locali, come orologi a controllo radio.

14.11.2 Configurazione nella rete

In SUSE LINUX, xntp è preconfigurato in modo che solo l'orario del sistema locale funge da ora di riferimento. Il modo più semplice di utilizzare dei server dell'ora nella rete consiste nell'indicazione dei cosiddetti parametri "server". Se nella rete vi è un server dell'orario che ad esempio ha il nome di `ntp.example.com` potete immettere questo server in `/etc/ntp.conf` nel modo seguente: `server ntp.example.com`.

Ulteriori server dell'ora vengono aggiunti 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 stabilizza e che viene creato il file "drift" per correggere l'orario del sistema locale. Il file "drift" visto a lungo termine presenta il vantaggio che già dopo aver acceso il computer si sa di quanto devia l'orario di sistema, e si procede immediatamente alla correzione dell'orario per cui si ha una elevata stabilità dell'orario del sistema.

Se nella vostra rete il server dell'ora è indirizzabile anche tramite un broadcast, non avete bisogno del nome del server. Potete configurarlo con il parametro `broadcastclient` anche nel file di configurazione `/etc/ntp.conf`. In questo caso si consiglia comunque di configurare un meccanismo di autenticazione, poiché un server dell'ora con degli errori andrebbe ad influire sull'orario del vostro sistema.

xntpd può essere solitamente indirizzato nella rete anche come server dell'ora. Se volete utilizzare xntpd anche tramite broadcast, configurate l'opzione `broadcast`:

```
broadcast 192.168.0.255
```

Chiaramente qui dovete immettere il vostro indirizzo broadcast effettivo. Assicuratevi che il server dell'ora utilizzi effettivamente l'ora esatta. A tal fine si consigliano degli orari di riferimento.

14.11.3 Impostare un orario di riferimento locale

Il pacchetto programma `xntp` contiene anche dei driver che permettono di impostare l'ora di riferimento locale. Gli orologi supportati si trovano nel pacchetto xntp-doc nel file `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. Gli orologi vengono registrati nel file `/etc/ntp.conf`, come se si trattasse di orologi disponibili nella rete.

A riguardo gli vengono assegnati degli indirizzi IP particolari simili a: `127.127.t.u`. Il valore `t` si ottiene dal file sovramenzionato con l'elenco degli orologi di riferimento. `u` è il numero di dispositivo che è diverso da 0 solo se utilizzate diversi orologi dello stesso tipo sul vostro sistema. `Type 8 Generic Reference Driver (PARSE)` avrebbe quindi lo pseudo indirizzo IP `127.127.8.0`.

I singoli driver di solito hanno dei parametri speciali che descrivono la configurazione in modo più dettagliata. Nel file `file:/usr/share/doc/packages/xntp-doc/html/refclock.htm` trovate inoltre per ogni driver un link alla relativa pagina driver che descrive il parametro. Per orologi del tipo 8 ad esempio è necessario indicare un ulteriore cosiddetto mode che specifica meglio l'orologio. Per esempio il modulo `Conrad DCF77 receiver module` presenta il mode 5. Affinché questo orologio sia preso da xntp come riferimento aggiungete inoltre la parola chiave `prefer`. La riga `server` completa di un "Conrad DCF77 receiver module" è quindi:

```
server 127.127.8.0 mode 5 prefer
```

Per gli altri orologi 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 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*.

15.1 I principi

15.1.1 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).

15.1.2 HTTP

Spesso i client sono dei browser web come Konqueror o Mozilla. Il browser e il server web comunicano tramite l'*H* yper *T*ext *T*ransfer *P*rotocol (HTTP). (La documentazione relativa all'attuale versione HTTP 1.1 e reperibile nell' RFC 2068 così come nell'Update RFC 2616. Gli RFC sono li trovate al seguente indirizzo URL: `http://www.w3.org`

15.1.3 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:

- Un protocollo. I protocolli di maggior diffusione sono
  - `http://` Il protocollo HTTP.
  - `https://`La versione sicura e criptata di HTTP.
  - `ftp://` *F*ile *T*ransfer *P*rotocol per eseguire il download ed l'upload di file.
- Un dominio, in questo caso `www.suse.de`. Il dominio è composto a sua volta da una prima parte (`www` che rimanda ad un computer, e da una seconda parte `suse.de` che rappresenta il dominio vero e proprio. La prima parte e la seconda parte compongono insieme il Fully Qualified Domain Name (spesso abbreviato con FQDN) che in italiano potremmo chiamare: nome di dominio completo.
- Una risorsa, in questo caso `index.html`. Questa sezione ne indica il percorso completo. 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.de` viene realizzato dai relativi meccanismi dell' Internet (p.e.Domain Name System, DNS), che inoltrano la richiesta di accesso al dominio ad uno o più computer di competenza. Apache fornisce poi la risorsa, nel nostro caso si tratta semplicemente della pagina (`index.html`) presa dalla sua directory di file. In questo caso il file si trova nel primo livello della directory ma potrebbe trovarsi anche in una sottodirectory, ad esempio `www.suse.de/business/services/support/index.html`

Il percorso del file viene specificato nella cosiddetta DocumentRoot che può essere modificato nei file di configurazione, come descritto nella sezione 15.7.2 a pagina 394.

15.1.4 Output automatico 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 se Apache debba servirsi di questo automatismo, e stabilire quali pagine includere come descritto nella sezione 15.7.2 a pagina 395. Nel nostro esempio, immettendo `http://www.suse.de` il server fornirà la pagina `http://www.suse.de/index.html`.

15.2 Configurare il server HTTP con YaST

Apache 2 può essere configurato in modo veloce e semplice con YaST. Comunque doveste disporre delle nozioni fondamentali se intendete impostare un server web. Se nel centro di controllo (Control Center) di YaST andate su 'Servizi di rete' -> 'Server HTTP', eventualmente vi sarà chiesto se, YaST debba installare i pacchetti mancanti. Se quanto richiesto è installato arrivate la dialogo di configurazione.

Abilitate qui il servizio HTTP. Di default vi sono tre opzioni: 'Nome server', 'E-Mail dell'amministratore del server' ed 'Ascolta su'. Per l'ultima opzione è già impostata la porta 80. Tramite il bottone 'Aggiungi' potete selezionare ulteriori opzioni. Con 'Modifica' potete intervenire sul valore della opzione selezionata, 'Cancella' rimuove l'opzione.

Tramite la combo-box 'Per esperti' potete selezionare 'Visualizzare protocollo di accesso', 'Visualizzare protocollo degli errori' e configurare i 'Moduli server' da caricare per il server. In questa maschera abilitate e disabilitate i moduli tramite il pulsante 'Modifica stato' e potete aggiungere dei moduli tramite 'Aggiungi modulo'.

15.3 I moduli di Apache

Tramite dei moduli potete integrare in Apache numerose funzionalità. Per esempio attraverso dei moduli, Apache potrà eseguire script CGI nei più svariati 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 vedi la sezione 15.13.4 a pagina 411

Per l'elaborazione di richieste, Apache utilizza uno o più "handler" (che vengono indicati tramite delle direttive nel file di configurazione). Questi handler possono essere parte integrante di Apache oppure si può lanciare un modulo per l'elaborazione della richiesta. In tal modo questo processo si lascia realizzare in modo flessibile. 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 particolar modo per quel che riguarda Apache 2 il concetto di modularizzazione è stato esteso notevolmente, qui il server svolge solo una funzione minimale ed il resto viene realizzato tramite dei moduli. Per fare un esempio in Apache 2 persino il processo di elaborazione di HTTP viene realizzato tramite dei moduli. Apache 2 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 "proof-of-concept" mail server (POP3) basato su Apache.

Apache supporta una serie di utili feature di cui segue una breve rassegna.

Host virtuali Il supporto di host virtuali consente che con una istanza di Apache su di un singolo server possono essere gestiti 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. Nel caso degli host virtuali vi è la configurazione basata sull'indirizzo IP oppure quella basata sul nome. Grazie all'hosting virtuale potete risparmiarvi i costi d'acquisto ed i costi derivanti dall'amministrazione di ulteriori computer.

Riscrittura flessibile delle URL Apache offre una serie di possibilità di 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 volete imbacarvi nell'impresa di adattare il codice JavaScript ad ogni 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 e rispondere in modo adeguato. Tramite CGI p. es., potrete comporre attivamente una risposta.

15.4 Le novità di Apache 2

Segue un elenco delle novità di Apache 2. La documentazione esaustiva relativa ad Apache HTTP Server Version 2.0 è reperibile alla seguente URL: `http://httpd.apache.org/docs-2.0/en/` in lingua inglese.

- Nel modo di processare contemporaneamente diverse richieste si ha la scelta tra cosiddetti thread e processi. I processi vengono amministrati da un apposito modulo, il cosiddetto modulo multi-processing (MPM). Il modo di rispondere di Apache 2 alle richieste viene determinato dal tipo di MPM. Ciò ha degli effetti soprattutto per quel che riguarda la performance e l'utilizzo dei moduli, come illustreremo di seguito.
- Apache utilizza adesso una propria libreria di base nuova (la cosiddetta Apache Portable Runtime, abbrev. con APR) quale interfaccia

per le funzionalità del sistema e gestione della memoria. Inoltre, è stata migliorata l'integrazione in Apache di moduli importanti e diffusi come mod_gzip (succede a : mod_deflate) oppure mod_ssl, che intervengono in modo non trascurabile sul processo di elaborazione delle richieste.

- Apache 2 supporta il protocollo Internet del futuro IPv6.
- Vi sono adesso dei meccanismi che permettono ai produttori di moduli di poter dare delle indicazione per quel che riguarda la sequenza nella quale debbano essere caricati i moduli, risparmiando all'utente di doversene occupare. La sequenza nella quale vengono eseguiti i moduli, che prima doveva venir stabilita dall'utente, ha una sua importanza. Così per esempio un modulo che permette l'accesso ad una determinata risorsa solo agli utenti autenticati deve essere caricato per primo, per evitare che degli utenti sprovvisti del permesso di accesso possano visualizzare la pagina in questione.
- Le richieste rivolte ad Apache e le risposte inviate da Apache possono essere filtrate.
- Supporto di file di oltre 2 GiB (Large-File-Support, LFS), su sistemi a 32 bit.
- Vi sono dei nuovi moduli che sono disponibili solo per Apache 2.
- Comunicazioni di errore multilingue

15.5 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. 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" cioè la funzione con lo stesso input deve produrre sempre lo stesso risultato, indipendentemente dal numero di thread in esecuzione. 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 come processi propri 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 (vedi la sezione 15.6) l'MPM da utilizzare. Lo sviluppo del terzo modo, "perchild", non è ancora del tutto concluso, così non è (ancora) disponibile in SUSE LINUX.

15.6 Installazione

15.6.1 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 che fa per voi dovete considerare che l'MPM worker non può essere utilizzato assieme al pacchetto `mod_php4`, dato che non tutte le librerie a cui ricorre questo pacchetto sono threadsafe.

15.6.2 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 l'URL `http://localhost/` in un browser. Se Apache è in esecuzione vedrete una pagina esempio, sempre se il pacchetto `apache2-example-pages` è stato installato.

15.6.3 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 è illustrato nella sezione 15.9.5 a pagina 401.

15.6.4 Altri pacchetti utili

Inoltre è consigliabile installare la corposa documentazione che trovate nel pacchetto `apache2-doc`. Per la documentazione vi è un alias (di cosa si tratta viene descritto nella sezione 15.7 a fronte), in modo da poter invocare la documentazione, dopo l'installazione, direttamente per via dell'URL `http://localhost/manual`.

Coloro che sviluppano dei moduli per Apache oppure che intendono 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 15.6.5.

15.6.5 Installare 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.

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/`.

L'opzione `-a` non dovrebbe venir utilizzata con Apache 2 dato che le modifiche vengono scritte direttamente in `/etc/httpd/httpd.conf`. Si consiglia invece di abilitare i moduli tramite la voce `APACHE_MODULES` che trovate sotto `/etc/sysconfig/apache2/`, come descritto nella sezione 15.7.1 a fronte.

15.7 Configurazione

Dopo aver installato Apache dovete intervenire sulla configurazione solo se avete delle esigenze o preferenze particolari. Apache si lascia configurare tramite SuSEconfig oppure editando direttamente il file `/etc/httpd/httpd.conf/`.

15.7.1 Configurazione con SuSEconfig

Le impostazioni che potete effettuare sotto `/etc/sysconfig/apache2`, vengono scritti tramite 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/httpd/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/httpd/httpd.conf` viene sovrascritto durante una reinstallazione.

Moduli

I moduli installati tramite YaST si abilitano immettendo il nome del modulo nella lista della 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.

15.7.2 Configurazione manuale

Il file di configurazione

Il file di configurazione /etc/apache2/httpd.conf consente di apportare delle modifiche che non è possibile 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. É impostata su /srv/www/htdocs per il default virtual host e di solito non è necessario apportare delle modifiche.

Timeout

Indica il tempo che il server fa trascorrere prima di comunicare un timeout (tempo scaduto) 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. In Apache 2 la sequenza di caricamento viene stabilita invece dai moduli, vedi a riguardo la sezione 15.4 a pagina 389. Inoltre, le direttive indicano i file contenuti dal modulo.

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 su 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 `DocumentRoot` esiste una tale direttiva, il nome di directory lì indicato deve essere modificato sempre in parallelo con `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 chiama l'URL `http://www.xyz.com/foo/bar` e sotto la DocumentRoot vi è una directory `foo/bar` che contiene il file `index.html`, Apache fornirà questa pagina al client.

AllowOverride

Ogni directory da cui Apache fornisce dei documenti può contenere un file che può modificare i permessi di accesso impostati globalmente ed altre impostazioni che interessano la directory in questione. Queste impostazioni sono ricorsive, cioè 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 le impostazioni di un file del genere in `DocumentRoot` hanno validità globale. Questi file di solito hanno il nome `.htaccess`, che potrete comunque cambiare, vedi a riguardo la sezione 15.7.2 nella pagina seguente.

Con `AllowOverride` si stabilisce se le impostazioni indicate nei file locali possano sovrascrivere le 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 tutti gli accessi, le eccezioni sono definite

deny all tutti gli accessi negati fatta eccezione per quelli definiti.

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 con permesso di sovrascrivere le impostazioni globali riguardanti i permessi di accesso etc., delle directory fornite da Apache (vedi anche la sezione 15.7.2 nella pagina precedente). 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 (vedi la sezione 15.10 a pagina 405) si trovano in questo file se nella sezione dedicata al VirtualHost del file di configurazione non è stato indicato un altro file di log.

LogLevel

I messaggi di errore sono suddivisi - in base all'urgenza - in diversi livelli. Qui potete impostare a partire da quale livello di urgenza emettere il messaggio. Verranno emessi i messaggi del livello impostato e quelli dei livelli superiori in termini di urgenza. 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`. (Finché la DocumentRoot ha questo valore non fa differenza.) Nel caso di questo alias con `http://localhost/manual` si accede direttamente alla directory relativa. Eventualmente dovrete indicare una direttiva `Directory`, con i permessi della directory, per la directory meta indicata nella direttiva `Alias` (vd. a riguardo la sezione 15.7.2 a pagina 395).

ScriptAlias

Questa direttiva è simile a quella Alias, comportando inoltre che i file nella directory meta vengano 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/httpd/suse_public_html.conf` (che viene letto da `/etc/httpd/httpd.conf`) si avrà una registrazione del tipo:

```
<IfModule mod_userdir.c>
UserDir public_html
</IfModule>
```

15.8 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; questi file possono essere sovrascritti (meglio: cancellarli). 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`. Lì viene documentata l'ora ed il metodo (`GET`, `POST`...) con il quale sono state richieste e messe a disposizione le risorse. In caso di errore trovate le indicazioni attinenti nel file `/var/log/apache2`.

15.9 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

alla elaborazione di 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)
Qui vengono eseguiti dei programmi che risiedono all'interno di determinate directory. Apache consegna a questi programmi i parametri trasmessi dal client, e riconsegna l'output del programma al client. Questo modo di programmare è relativamente semplice, anche perché si possono modificare i tool della riga di comando esistenti in modo che accettino dell'input di Apache e che gli ritornano l'output.

Moduli Apache offre delle interfacce per poter eseguire dei moduli come parte del processo di elaborazione, ed inoltre consente a questi programmi di accedere ad informazioni importanti come la request o l'intestazione 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 assumersi altre funzioni (p.e.autenticazione). Programmare questo tipo di moduli richiede una certa abilità; i vantaggi che ne conseguono sono alte prestazioni e possibilità che superano di molto quanto offerto dagli SSI e CGI.

Mentre gli script CGI vengono eseguiti quando invocati da Apache (con l'ID dell'utente del loro proprietario), coi moduli viene utilizzato un interprete embedded in Apache che sotto l'ID del server web è permanentemente in esecuzione. L'interprete si dice è "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 e della memoria), lo script invece viene semplicemente consegnato all'interprete già in esecuzione.

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 la negazione di 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 o eventi simili.

15.9.1 Server Side Includes:SSI

Server Side Includes sono delle direttive embedded in commenti particolari che vengono 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 degli 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 15.7.2 a pagina 397.

15.9.2 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 mette a disposizione 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 ritorna in risposta una pagina personalizzata in base alla richiesta.

Il più grande vantaggio della CGI sta nella sua semplicità. Il programma deve solo trovarsi in una determinata directory, e il server web lo eseguirà proprio alla stregua di un programma sulla riga di comando. L'output del programma sul canale standard di emissione (`stdout`) viene consegnato dal server semplicemente al client.

15.9.3 GET e POST

I parametri di immissione possono essere consegnati al server con `GET` oppure con `POST`. Il modo in cui il server consegna i parametri allo script dipende dal metodo utilizzato. Nel caso di `POST` il server consegna 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` i parametri vengono consegnati dal server al programma tramite la variabile di ambiente `QUERY_STRING`. Una variabile di ambiente è una variabile disponibile su tutto il sistema; un esempio ne è la variabile `PATH` che contiene una lista di percorsi in cui il sistema esegue le sue ricerche di comandi eseguibili ogni volta che l'utente digita un comando.

15.9.4 Linguaggi per CGI

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; per CGI dove l'accento è posto 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, vedi la sezione 15.7 a pagina 393.

Inoltre si possono stabilire ulteriori directory in cui Apache esegue le sue ricerche di programmi eseguibili. Questo comporta un certo rischio in termini di sicurezza, visto che ogni utente (malintenzionato) è in grado di far eseguire dei programmi da Apache.Se i programmi eseguibili vengono raccolti solo in `cgi-bin` l'amministratore può controllare più facilmente quali script e programmi deporvi, e se eventualmente si tratta di file che possono arrecare danno.

15.9.5 Creare contenuti dinamici tramite moduli

Vi sono una serie di moduli per Apache. Tutti i moduli descritti di seguito sono disponibili sotto forma di pacchetti in SUSE LINUX. Il termine modulo ha in questa sede 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 per integrare 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 ed emettere del codice HTML.

15.9.6 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 (vedi la sezione 15.6 a pagina 391). Le registrazioni necessarie per Apache sono già incluse nel file di configurazione, vedi `/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 e per `mod_perl`:

```
<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 mantenuti 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 rimangono 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 ad avviare 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 di variabili e nomi di routine definiti dall'esistenza di 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 a discapito della velocità, ma è comunque più veloce di CGI visto che non bisogna lanciare un processo per l'interprete. `Apache::PerlRun` si comporta alla stregua di CGI.

15.9.7 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 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 inoltre il pacchetto `apache2-mod_php4` .

15.9.8 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.

Per saperne di più, visitate il sito `http://www.python.org/`.Per maggior informazioni su `mod_python` andate su `http://www.modpython.org/`.

15.9.9 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 fa pensare a 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/`.

15.10 Host virtuali

Grazie agli host virtuali con un solo server web si possono gestire più domini, risparmiandosi in tal modo spese e lavoro di manutenzione dovuti ad un server per ogni dominio. Apache è stato uno dei primi server web a supportare questa caratteristica, e offre una serie di possibilità in tema di hosting virtuale:

- Hosting virtuale basato su nome
- Hosting virtuale basato sull'IP
- Eseguire diverse istanze di Apache su una macchina.

15.10.1 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/httpd/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 di devono configurare i singoli host virtuali:

```
<VirtualHost *>
    ServerName www.aziendauno.it
    DocumentRoot /srv/www/htdocs/aziendauno.it
    ServerAdmin webmaster@aziendauno.it
    ErrorLog /var/log/httpd/www.aziendauno.it-error_log
    CustomLog /var/log/httpd/www.aziendauno.it-access_log common
</VirtualHost>

<VirtualHost *>
    ServerName www.aziendadue.it
    DocumentRoot /srv/www/htdocs/aziendadue.it
    ServerAdmin webmaster@aziendadue.it
    ErrorLog /var/log/httpd/www.aziendadue.it-error_log
    CustomLog /var/log/httpd/www.aziendadue.it-access_log common
</VirtualHost>
```

Con Apache 2 il percorso per i file di log si dovrebbe modificare da `/var/log/httpd` a `/var/log/apache2`. Anche per il dominio ospitato originariamente dal server (`www.aziendauno.it` deve esservi una registrazione VirtualHost. Nel nostro esempio, lo stesso server gestisce accanto la domino originario un secondo dominio (`www.aziendadue.it`.

Anche nelle direttive `VirtualHost`, come nel caso di `NameVirtualHost`, viene indicato 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` corrisponda al nome host indicato in questo 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.

`Serveradmin` indica l'indirizzo e-mail dell' amministratore a cui rivolgersi in caso di problemi. Se si verificano degli errori Apache indicherà questo indirizzo nella comunicazione di errore che invia al client.

15.10.2 Hosting virtuale basato sull'IP

In questo caso bisogna impostare diversi IP su di un 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 che ospita 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 l'impostatazione 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 la macchina 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

```
/sbin/ifconfig eth0:0 192.168.1.20
/sbin/ifconfig eth0:1 192.168.1.21
```

Gli indirizzi IP vanno assegnati allo stesso 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.aziendadue.it
    DocumentRoot /srv/www/htdocs/aziendadue.it
    ServerAdmin webmaster@aziendadue.it
    ErrorLog /var/log/httpd/www.aziendadue.it-error_log
    CustomLog /var/log/httpd/www.aziendadue.it-access_log common
</VirtualHost>

<VirtualHost 192.168.1.21>
    ServerName www.aziendatre.it
    DocumentRoot /srv/www/htdocs/aziendatre.it
    ServerAdmin webmaster@aziendatre.it
    ErrorLog /var/log/httpd/www.aziendatre.it-error_log
    CustomLog /var/log/httpd/www.aziendatre.it-access_log common
</VirtualHost>
```

Qui si indicano le direttive VirtualHost per ulteriori domini, il dominio originario (`www.aziendauno.it` viene configurato attraverso le relative impostazioni (`DocumentRoot` etc.) all'infuori dei blocchi `VirtualHost`.

15.10.3 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` etc. 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
```

15.11 Sicurezza

15.11.1 Ridurre i rischi

Se il server web non vi serve, si dovrebbe disabilitare Apache nell' editor dei runlevel oppure non installarlo 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.

15.11.2 Permessi di accesso

Root dovrebbe essere il proprietario della 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, 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 deporvi i suoi file per presentazioni web (p.e. `~/public_html`). In SUSE LINUX questa funzionalità è abilitata di default, per ulteriori dettagli rimandiamo alla sezione 15.7.2 a pagina 398.

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.

15.11.3 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 15.13.3 nella pagina seguente sono elencate le fonti per exploit e bug-fix.

15.12 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/httpd/error_log` o `/var/log/apache2/error_log`.

  Una altra possibilità consiste nel seguire contemporaneamente i file di log in una console per vedere come reagisce il 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 le avete provate tutte senza risolvere il problema, e siete sicuri di trovarvi di fronte ad un baco di Apache, rivolgetevi direttamente a `http://www.suse.de/feedback/`.

15.13 Ulteriore documentazione

15.13.1 Apache

Apache dispone di una documentazione esaustiva, come installarla sul vostro sistema viene descritto nella sezione 15.6 a pagina 391. La troverete in seguito sotto `http://localhost/manual`. La documentazione aggiornata chiaramente la troverete sempre sulla home page di Apache: `http://httpd.apache.org`

15.13.2 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.modpercookbook.org/`
- `http://www.fastcgi.com/`
- `http://www.boutell.com/cgic/`

15.13.3 Sicurezza

Sotto `http://www.suse.de/security/` trovate sempre le patch attuali per pacchetti SUSE da poter scaricare. Visitate regolarmente questa URL, qui potrete anche abbonarvi tramite mailing list ai Security Announcements SUSE.

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/`

15.13.4 Ulteriori fonti

Nel caso incontraste delle difficoltà, vale la pena consultare la banca dati di supporto della SuSE (in lingua inglese):`http://sdb.suse.de/en`

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.

Sincronazzazione dei file

Oggi sono in tanti a utilizzare e 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 usa durante gli spostamenti. Molti file devono essere presenti su tutti quanti i computer, così da poter svolgere il proprio lavoro indipendentemente dal computer che si ha davanti e poter in particolar modo modificare i dati. E chiaramente tutti i dati devono essere disponibili nella versione attuale su ognuno dei differenti computer.

16.1 Software per la sincronizzazione dei dati

Nel caso di computer collegati costantemente tramite una rete veloce la sincronizzazione dei dati non rappresenta un problema. Si seleziona un file system di rete, per esempio NFS e si salvano i file su un server. I vari computer accedono poi tramite rete agli stessi e identici dati sul server.

Questo approccio non è possibile se la rete è molto lenta o se addirittura è in parte inesistente. Chi usa un laptop durante i suoi spostamenti necessità assolutamente delle copie dei file da elaborare sul proprio disco rigido locale. Non appena però si inizia ad 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. Comunque nel caso di numerosi file il tutto diventa già più laborioso e richiede molta attenzione per evitare che si sovrascriva per esempio un file nuovo con la versione antecedente.

Attenzione

Occhio alla perdita di dati

In ogni caso bisogna sapere usare bene il programma utilizzato 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.

Attenzione

Per risparmiarsi queste procedure laboriose che portano via tanto tempo prezioso e soggette ad errori vi è del software che seguendo approcci diversi automatizza questo lavoro.

Il supporto all'installazione della SuSE NON copre anche i programmi descritti in questo capitolo. 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.

16.1.1 InterMezzo

L'idea che sta alla base di InterMezzo è quella di costruire un file system che permetta di scambiare i dati tramite rete come l'NFS e contemporaneamente di salvare su ogni computer delle copie locali, in modo che

anche nel caso della caduta della connessione di rete i file siano comunque disponibili. Si può continuare a editare le copie locali dato che un file protocollo speciale annota tutte le modifiche. Quando viene ristabilita la connessione, le modifiche vengono inoltrate automaticamente ed i file sincronizzati. Per avere ulteriori informazioni su InterMezzo leggete l'howto `/usr/share/doc/packages/InterMezzo/InterMezzo-HOWTO.html` ; per farlo il pacchetto deve essere chiaramente installato.

16.1.2 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 viene creata una banca dati nei due computer interessati nella quale vengono memorizzati le somme di controllo, la datazione e i permessi dei file selezionati.

Alla prossima chiamata unison è in grado di riconoscere quali file hanno subito delle modifiche e propone la trasmissione da un computer o verso un computer. Solitamente potrete accettare tranquillamente le proposte di unison.

16.1.3 CVS

Impiegato soprattutto per l'amministrazione delle varie versioni dei sorgenti di programmi il CVS consente di avere delle copie dei file su diversi computer. In questo senso è adattato anche al nostro scopo.

Il CVS ha un database centrale chiamato repository che risiede sul server che memorizza non solo i file ma anche le singole modifiche apportate ai file. Le modifiche eseguite in locale vengono immesse nel database, si parla di commit, e così possono essere scaricate dagli altri computer (update). Entrambi i processi devono essere eseguiti dall'utente.

Il CVS si rivela essere molto tollerante nei confronti di errori per quanto riguarda le modifiche effettuate da diversi computer: le modifiche vengono accolte 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.

16.1.4 mailsync

A differenza dei tool di sincronizzazione finora menzionati, Mailsync è atto solo alla sincronizzazione delle 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 cancellarla o sincrolizzarla.

E' possibile sincronizzare sia singole mail box sia gerarchie di mail box.

16.2 Criteri per scegliere il programma giusto

16.2.1 Client-Server vs. parità

Per la sincronizzazione dei dati si sono diffusi principalmente due modelli. Nel primo caso vi è un server centrale in base al quale i client cioè gli altri computer sincronizzano i loro file. I client dovranno potersi collegare tramite una rete almeno ad certi intervalli di tempo al server. Questo modello è quello utilizzato dal CVS ed InterMezzo.

L'alternativa è rappresentata da computer "equiparati" e che sincronizzano i loro dati a vicenda. Questo è l'approccio che segue unison.

16.2.2 Portabilità

InterMezzo è una soluzione che al momento funziona solo su sistemi Linux. In passato funzionava solamente su architetture little-endian (ix86) a 32 bit. Con il passaggio da lento che si basa su perl a InterSync questa restrizione è stata superata. Comunque quando sincronizzate dei dati residenti su diverse architteture dovete fare attenzione, poiché si tratta di una feature poco testata.

cvs e unison sono disponibili anche per tanti altri sistemi operativi come la famiglia Unix e Windows.

16.2.3 Interattivo vs. automatico

Nel caso di InterMezzo la sincronizzazione dei dati avviene di solito automaticamente in background, non appena si effettua il collegamento tramite rete al server. Solo nel caso si verifichino dei conflitti è necessario intervenire.

Con cvs e unison la sincronizzazione viene iniziata 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 possibilità del verificarsi dei conflitti.

16.2.4 Velocità

unison e cvs vista l'interattività sembrano più lenti rispetto a intermezzo che lavora in background. cvs è in linea di massima un pò più veloce di unison.

16.2.5 Il verificarsi e la risoluzione di conflitti

In cvs i conflitti si verificano solo raramente anche se sono diverse persone a collaborare 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 cvs i conflitti sono semplici da risolvere.

unison comunica il verificarsi di conflitti e si può escludere il file dalla sincronizzazione. Non è così semplice allinerare le modifiche come nel caso del cvs.

Visto che non vi è interattività con InterMezzo i conflitti non si lasciano risolvere interattivamente. Nel caso di conflitti InterSync emmette un messaggio che avverte della presenza di un conflitto. In questi casi è l'amministratore di sistema che deve intervenire ed eventualmente eseguire a mano un rsync/scp) per ottenere la consistenza dei dati.

16.2.6 Selezione dei file e aggiunta di file

InterMezzo sincronizza l'intero file system. Nuovi file all'interno di un file system compaiono automaticamente sugli altri computer.

Nella configurazione più semplice di unison viene sincronizzato un intero albero di directory. I file che si aggiungono all'albero vengono sincronizzati automaticamtente.

In CVS bisogna aggiungere esplicitamente nuovi file e directory tramite il comando `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 cvs update si ignorano i '?' a causa del mole dei file.

16.2.7 Lo storico

cvs permette inoltre di ricostruire versioni precedenti di un file. Ad ogni modifica si ha la possibilità di 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 della tesi o dei sorgenti di un programma.

16.2.8 Volume dei dati e spazio richiesto sul disco rigido

Su ogni computer interessato serve abbastanza spazio per i dati dislocati.

Per il cvs serve inoltre del 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 nel formato 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.

16.2.9 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 Windows (wincvs). Tanti tool di sviluppo (p.es. kdevelop) ed editor di testo (p.es. emacs) supportano CVS. Grazie a questi front-end risolvere dei conflitti diventa una faccenda davvero semplice.

InterMezzo non offre tutte queste comodità. Dall'altra parte comunque solitamente non vi è alcun bisogno di interagire visto che dopo esser stato installato InterMezzo dovrebbe assolvere al suo compito in background.

16.2.10 Cosa viene richiesto dall'utente

L'installazione di InterMezzo non è un'impresa semplicissima e dovrebbe essere eseguita da un amministratore di sistema che ha già un pò di esperienza in ambito Linux. Per l'installazione servono i privileggi di `root`.

unison è semplice da utilizzare ed è appropriato anche per principianti.

CVS è già un pò più difficile da utilizzare. Prima di impiegarlo si dovrebbe aver afferrato il modo di interazione 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`. Dopo aver eseguito questo comando, con il comando `cvs commit` i dati vanno rispediti nel repository. Se ci si attiene sempre a questa procedure il CVS risulta essere semplice da utilizzare anche per dei principianti.

16.2.11 Sicurezza contro attacchi

La sicurezza contro l'intercettazione o addirittura la manipolazione dei dati durante il loro trasferimento dovrebbe essere sempre data.

Sia per unison che cvs si può ricorrere ad ssh (Secure Shell) per mettersi al riparo dagli attacchi sovramenzionati. 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.

InterMezzo utilizza http per la sincronizzazione dei dati. Questo protocollo è facile da intercettare o falsificare. Per aumentare il grado di sicurezza, si può utilizzare SSL che però rende la configurazione un pò più complessa. Senza SSL si dovrebbe utilizzare InterMezzo solo in reti protette e affidabili.

16.2.12 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).

unison è un prodotto relativamente nuovo ma è molto stabile. E' più esposto ad errori dovuti all'utente: se si accetta di cancellare un file durante il processo di sincronizzazione, il file risulta irrimediabilemte perduto.

InterMezzo si trova al momento in stato sperimentale. Dato che i file vengono memorizzati in un file system sottostante la possibilità che si verifichi

una perdita di dati è relativamente bassa. Però può verificarsi un errore durante la sincronizzazione dei dati e corrompere dei file. Anche per quanto riguarda la tolleranza nei confronti di errori dovuti all'utente è bassa: se si cancella localemente un file, ciò verrà applicato anche su tutti gli altri computer sincronizzati. Per tale ragione si consiglia caldamente di fare delle copie di sicurezza, i cosiddetti back-up.

Tabella 16.1: *Feature dei tool di sincronizzazione -- = molto scarso, - = scarso o non presente, o = mediocre, + = buono, ++ = molto buona, x = presente*

	InterMezzo	unison	CVS	mailsync
CS/parità	C-S	pari	C-S	pari
Portabil.	Linux(i386)	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x
Interattiv	-	x	x	-
Velocità	++	-	o	+
Conflitti	-	o	++	+
Selez,file	Filesystem	Directory	Selezione	Mailbox
Storico	-	-	x	-
Spazio	o	o	--	+
GUI	-	+	o	-
Difficolt.	-	+	o	o
Attacchi	-	+(ssh)	+(ssh)	+(SSL)
Perd.dati	o	+	++	+

16.3 Introduzione ad Inter-Mezzo

16.3.1 Architettura

Nel caso di InterMezzo si tratta di un tipo di file system a sé stante. I file vengono memorizzati su ogni computer localmente sul disco rigido. Per fare ciò viene utilizzato uno dei filesystem di Linux, preferibilmente `ext3` o un altro journaling file system. Dopo aver preparato la partizione viene

montato il file system di tipo `intermezzo`. Il kernel carica un modulo con il supporto per InterMezzo e d'ora in poi le modifiche fatte in questo file system vengono scritte in un file protocollo, i cosiddetti log file.

A questo punto si può avviare InterSync che a sua volta inizializza un server web,e.g. apache, a cui hanno accesso anche altri computer per scambiarsi i dati. Quando configurate un client bisogna comunicare ad InterSync il nome del server, che viene contattato. Per il riconoscimento del file system viene passata una denominazione liberamente scelta per il file system, il fileset.

InterSync è la nuova versione di InterMezzo che utilizzava un daemon scitto in Perl di nome lento per la sincronizzazione dei dati. Nella documentazione di InterSync a volte vi sono dei riferimenti a questo sistema più vecchioto, al cui posto è subentrato InterSync. Il modulo del kernel standard purtroppo non è al livello di lento e non funziona con InterSync. Il kernel SUSE comunque contiene un modulo più recente. Se volete compilarvi un kernel da voi si dovrebbe compilare il modulo del kernel con il pacchetto km_intersync.

Per installare e configurare InterMezzo sono richiesti i privileggi dell'amministratore. Come visto sopra amministrare InterMezzo non è del tutto semplice e dovrebbe essere fatto da amministratori di sistema già con una certa esperienza. La configurazione descritta di seguito non prevede alcun meccanismo di protezione, il che significa che chiunque (malintenzionato) nella rete ha possibilità di intercettare e manipolare i vostri dati sincronizzati tramite InterMezzo. Si dovrebbe configurare il programma in un ambiente sicuro e.g. in una rete collegata via cavo protetta da un firewall.

16.3.2 Configurare un server InterMezzo

Uno dei computer, preferibilmente uno con una buona connessione di rete svolgerà il ruolo di server. Tutto lo scambio di dati per la sincronizzazione dei dati si svolge tramite esso.

Per poter salvare i dati bisogna configurare un proprio file system. Se non si dispone più di alcuna partizione e non si utilizza l'LVM, questo file system si lascia realizzare semplicemente tramite un loop device. In questo caso un file nel file system locale assume il ruolo di un proprio file system.

Nel seguente esempio verrà creato un file system InterMezzo/ext3 di 256 Mbyte nella directory root. Il fileset verrà chiamato fset0.

```
dd if=/dev/zero of=/izo0 bs=1024 count=262144
mkizofs -r fset0 /izo0  # Questo avvertimento può essere ignorato
```

Questo file system adesso viene montato sotto `/var/cache/intermezzo`

```
mount -t intermezzo -ofileset=fset0,loop /izo /var/cache/intermezzo
```

In un secondo momento questo si può far eseguire automaticamente al boot con una registrazione nel file `/etc/fstab`. A questo punto bisogna configurare InterSync. A tale scopo va adattato `/etc/sysconfig/intersync`, immettendovi

```
INTERSYNC_CLIENT_OPTS="--fset=fset0"
INTERSYNC_CACHE=/var/cache/intermezzo
INTERSYNC_PROXY=""
```

Adesso si può avviare intersync con il comando

```
/etc/init.d/intersync start
```

Per automatizzare questo processo all'avvio del sistema immettete questo servizio nella lista dei servizi da avviare:

```
insserv intersync
```

16.3.3 Configurare un client InterMezzo

La configurazione dei client (un server può mettere a disposizione un servizio per diversi client) non si distingue molto da quella di un server. L'unica differenza è che quando si configura `/etc/sysconfig/intersync` alla variabile `INTERSYNC_CLIENT_OPTS` si deve indicare inoltre il nome del server:

```
INTERSYNC_CLIENT_OPTS="{}--fset=fset0 --server=sole.example.com"
```

Al posto di sole.example.com va naturalmente immesso il nome di rete del server. Si consiglia inoltre di creare dei file system della stessa dimensione su ogni computer.

16.3.4 Risoluzioni di problemi

Non appena viene avviato un client, le modifiche apportate ai file dovrebbero essere visibili sul server e su tutti gli altri client nella `/var/cache/intermezzo/`. Se non è così spesso la causa è da ricercare nel fatto che non vi è connessione al server o che vi è un errore di configurazione come, per fare un esempio, nomi diversi per il fileset. Ai fini della diagnosi è di sicuro aiuto analizzare le registrazioni nel file di log `/var/log/messages`. Il server web inizializzato protocolla i propri dati sotto `/var/intermezzo-X/`. I file di log del kernel che protocollano le modifiche apportate al file system si trova sotto `/var/cache/intermezzo/.intermezzo/fset0/kml` è può essere visualizzato tramite `kmlprint`.

Quando si verificano dei conflitti uno processo dei processi `InterSync` si ferma. Se la sincronizzazione dei dati non avviene più, si dovrebbero cercare delle indicazioni nei file di log e controllare con `/etc/init.d/intersync status` se il servizio di sincronizzazione è ancora in esecuzione.

Altrimenti consultate la documentazione del pacchetto:`/usr/share/doc/packages/intersync/`, `http://www.inter-mezzo.org/`.

16.4 Introduzione ad unison

16.4.1 Campi di applicazione

Unison si adatta perfettamente ai fini della sincronizzazione 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.

16.4.2 Presupposti

Unison deve essere installato sia sul client che sul server – con "server" si intende in questo caso un computer remoto (a differenza con CVS, vedi capitolo 6).

Nella seguente esposizione ci limiteremo all'impiego di unison in combinazione con ssh, dunque è necessario che sia installato un client ssh sul client ed un server ssh sul server.

16.4.3 Utilizzo

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: ammesso che abbiamo il seguente layout di directory:

Client:	`/home/tux/dir1`
Server:	`/home/geeko/dir2`

e vogliamo sincronizzare queste due 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 la relazione tra le due directory, e fa delle proposte per quando riguarda la direzione di trasferimento dei singoli file e directory. Le freccia nella colonna "Action" indicano la direzione di trasferimento. '?' significa che unison non riesce ad fare una proposta riguardo alla direzione di trasferimento, dato che entrambi le versioni nel frattempo o sono state modificate o aggiunte.

Con i tasti freccia si può impostare la direzione di trasferimento per ogni singola registrazione. Quando si ha la direzione di trasferimento giusta per le registrazioni visualizzati, allora si fa clic su "Go".

unison (p.es. se eseguire automaticamente la sincronizzazione nei casi chiari) può essere gestito all'avvio tramite parametri immessi sulla riga di comando. Un elenco completo dei parametri si ottiene con `unison -help`.

Per ogni collegamento vengono protocollati gli eventi di sincronizzazione nella directory dell'utente `~/.unison`. In questa directory si possono immettere anche i set di configurazione, e.g. `~/.unison/example.prefs`:

Exempio 16.1: *Il file /.unison/example.prefs*

```
root=/home/foobar/dir1
root=ssh://fbar@server//homes/fbar/dir2
batch=true
```

Per inizializzare la sincronizzazione basta semplicemente indicare il file come argomento della riga di comando: `unison example.prefs`

16.4.4 Ulteriore documentazione

La documentazione ufficiale su Unison non lascia nulla a desiderare, per questo ci siamo limitati ad una breve introduzione. Sotto `http://www.cis.upenn.edu/~bcpierce/unison/` o nel pacchetto SUSE `unison` troverete un manuale completo.

16.5 Introduzione a CVS

16.5.1 Campi di impiego

CVS può essere utilizzato anche ai fini della sincronizzazione, quando si modificano frequentemente singoli file nel formato di testo ASCII oppure sorgenti di programma). Con CVS si possono sincronizzare anche dati in altri formati (p.es. file JPEG), ma questo condurrà subito allo straripare del volume dei file, 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.

CVS si può utilizzare per la sincronizzazione dei dati solo se i computer sono tutti collegati allo stesso server !

Mentre con e.g. unison sarebbe pensabile anche questo scenario:

A > B > C > S

A, B, C sono computer che possono elaborare i dati in questione.

16.5.2 Impostare un server CVS

Sul server si trovano tutti i dati validi, ovvero soprattutto la versione attuale di ogni file. Anche e.g. una postazione di lavoro fissa può fungere da server. E' consigliabile eseguire regolarmente un back-up dei dati che risiedono sul server CVS.

Si rivela essere molto utile di avere un server CVS a cui gli utenti possono accedere tramite SSH, in tal modo una postazione di lavoro fissa p.es. può svolgere il ruolo di server.

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 (ciò deve avvenire solo una volta).

Infine bisogna stabilire un nome per la sincronizzazione. Per fare questo sul client bisogna andare in una directory che contiene file che devono essere amministrati esclusivamente dal CVS (può essere anche vuota). Il nome della directory non fa differenza ed nel nostro esempio utilizziamo il nome `synchome`. Per impostare il nome della sincronizzazione su `synchome`, si deve immettere:

```
cvs import synchome tux tux_0
```

Attenzione: Molti comandi del CVS richiedono un commento. A tale scopo il 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, e.g.

```
cvs import -m 'questa è una prova' synchome tux tux_0
```

16.5.3 Utilizzare il CVS

A partire da questo momento si può effettuare da un computer qualsiasi il check out dal repository di sincronizzazione :

```
cvs co synchome
```

Si avrà una nuova sottodirectory `synchome` sul client. Se si sono fatte delle modifiche che si vogliono comunicare al server, bisogna cambiare nella directory synchome (o anche in una sottodirectory di synchome) ed si immette il seguente comando:

```
cvs commit
```

Con questo comando vengono trasmessi al server tutti i file (incluse le sottodirectory).

Se si vuole eseguire il trasferimento solo di singoli file/directory, bisogna inidicarli esplicitamente:

```
cvs commit file1 ... directory1 ...
```

Prima di trasmettere nuovi file/directory al server bisogna aggiungerli al CVS nel modo seguente:

```
cvs add file1 ... directory1 ...
```

e dopo trasferirli con

```
cvs commit file1 ... directory1 ...
```

Se cambiate postazione di lavoro, dovrete se non lo avete già fatto durante sessioni di lavoro precedenti alla stessa postazione, eseguire il check out (vedi sopra) del repository di sincronizzazione.

La sincronizzazione con il server viene inizializzata tramite il seguente comando:

```
cvs update
```

Sussiste inoltre la possibilità di eseguire l'update di singoli file e directory:

```
cvs update file1 ... directory1 ...
```

Se volete vedere le differenze rispetto alle versioni memorizzate sul server, immettete

```
cvs diff
```

oppure

```
cvs diff file1 ... directory1 ...
```

In più avete anche la possibilità di farvi mostrare quali file verrebbero aggiornati (update):

```
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 senza essere stata aggiornata

P la versione locale è stata "patchata" ovvero adattata, cioè il CVS ha tentato di coniugare la versione che si trova sul server CVS con quella locale

? questo file non si trova nel CVS

`M` rappresenta un conflitto che va risolto. Le possibilità sono o trasmettere la copia locale al server, cioè eseguire un (commit) o si elimina la copia locale ed si esegue nuovamente un update - in tal modo il file mancante viene recuperato dal server.

16.5.4 Ulteriore documentazione

Le possibilità di impiego del CVS sono immense e noi abbiamo fornito solo una breve introduzione. La documentazione dettagliata si trova tra l'altro ai seguenti indirizzi: `http://www.cvshome.org/`, `http://www.gnu.org/manual/`

16.6 Introduzione a mailsync

16.6.1 Campo di impiego

Mailsync assolve principalmente a tre compiti:

- sincronizza e-mail localemente memorizzati con e-mail memorizzati su un server
- esegue la migrazione di mail box in un altro formato o su un altro server
- verifica l'integratà di una mail box o cerca i doppioni

16.6.2 Configurazione ed uso

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 scritta nel file `~/.mailsync`. Seguono alcuni esempi relativi agli store:

Una semplice definizione ha e.g. 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 richiama `mailsync` con

```
mailsync -m saved-messages
```

viene elencato in saved-messages un indice con tutti i messaggi. Se si definisce

```
store localdir {
          pat     Mail/*
          prefix  Mail/
}
```

con

```
mailsync -m localdir
```

si avrà un elenco di tutti i messaggi memorizzati nelle cartelle sotto Mail/. Con

```
mailsync localdir
```

invece vengono elencati i nomi delle cartelle. La specificazione di uno store sul server IMAP p.es. ha il seguente aspetto:

```
store imapinbox {
  server  {mail.uni-hannover.de/user=gulliver}
  ref     {mail.uni-hannover.de}
  pat     INBOX
}
```

Nell'esempio riportato sopra viene indirizzato solo la cartella principale sul server IMAP, uno store per le sottodirectory invece assume il seguente aspetto:

```
store imapdir {
  server  {mail.uni-hannover.de/user=gulliver}
  ref     {mail.uni-hannover.de}
  pat     INBOX.*
  prefix  INBOX.
}
```

Se il server IMAP supporta le connessioni cifrate, le specificazioni del server si dovrebbero modificare in

```
server  {mail.uni-hannover.de/ssl/user=gulliver}
```

o (se non conoscete il certifcato del server) in

```
server {mail.uni-hannover.de/ssl/novalidate-cert/user=gulliver}
```

Il prefisso viene spiegato successivamente.

A questo punto vanno collegate le cartelle sotto `Mail/` con le sottodirectory sul server IMAP:

```
channel cartella localdir imapdir {
        msinfo .mailsync.info
}
```

Mailsync registrerà nel file indicato con `msinfo` quali messaggi sono stati già sincronizzati.

```
mailsync cartella
```

procura che:

- pat (la mail box campione) venga applicato ad entrambi gli host
- venga eliminato il prefisso dai nomi delle cartelle che si creano durante il processo
- le cartelle vengano sincronizzate a due a due (o create se ancora non esistenti)

La cartella `INBOX.sent-mail` sul server IMAP viene sincronizzata con la cartella locale `Mail/sent-mail` (ciò presuppone la definizione di cui sopra). Quindi viene eseguita la sincronizzazione delle singole cartelle nel modo seguente:

- se il messaggio esiste su entrambi gli host non succede niente
- se 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 (visto che esisteva sull' altro host ed è stato cancellato lì)

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 in 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 in locale durante la sincronizzazione.

16.6.3 Possibili difficoltà

Nel caso che si verifichi una perdita di dati, il modo più sicuro di procedere quello è di cancellare i relativi file di protocollo channel msinfo. In tal modo tutti i messaggi che esistono solo da una parte sono considerati dei nuovi messaggi e verranno trasmessi alla prossima sincronizzazione.

Saranno presi in considerazione per quanto riguarda la sincronizzazione solo quei messaggi che hanno una cosiddetta message-id. I messaggi sprovvisti un tale identificativo verranno ignorate, i. e. non verranno né trasmessi né cancellati. Spesso la mancanza della message-id è dovuta ad errori nei programmi con i quali si consegna o si redige l'e-mail.

Su determinati server IMAP la cartella principale viene indirizzata tramite `INBOX`, e le sottodirectory tramite un nome qualsiasi (a differenza di INBOX ed INBOX.nome). In tal modo per questi server IMAP non è possibile specificare un modello esclusivamente per le sottodirectory.

I driver per mail box (c-client) utilizzati da Mailsync, dopo la trasmissione riuscita dei messaggi impostano sul server IMAP una speciale indicazione di stato (status flag) per cui alcuni programmi di e-mal come è il caso per mutt non riescono ad riconoscere i nuovi messaggi come tali. Per evitare che venga impostata una indicazione di stato, si usa l'opzione `-n`.

16.6.4 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".

Reti eterogenee

Linux non riesce solo a comunicare con altri computer Linux, ma anche con computer su cui gira Windows, Macintosh nonché tramite reti Novell. Questo capitolo vi mostra cosa dovete tenere sempre presente e come configurare reti eterogenee.

17.1 Samba

17.1.1 Samba: i principi

Con il pacchetto-programma Samba è possibile trasformare un qualsiasi computer Unix in un server di file e stampa performante per client DOS, Windows ed OS/2: il progetto Samba viene curato dal Samba Team ed è stato sviluppato dall'australiano Andrew Tridgell.

Samba è ormai un prodotto maturo, e per questo motivo in questo capitolo possiamo trattare brevemente solo alcune delle sue funzionalità. Comunque il software viene fornito con documentazione completa in forma digitale composta da una parte da pagine di manuale — a causa del volume dovete immettere `apropos samba` sulla riga di comando — ed dall'altra parte trovate ulteriore documentazione ed esempi sotto `/usr/share/doc/packages/samba`, dopo aver installato Samba. Nella sottodirectory `examples` trovate anche la configurazione esempio commentata `smb.conf.SuSE`.

A partire da SUSE LINUX 9.1 è a vostra disposizione il pacchetto `samba`, versione 3. Ecco alcune delle principali novità del pacchetto:

- Supporto Active Directory.
- Perfezionamento del supporto di Unicode.
- Rielaborazione completa dei meccanismi di autenticazione interni.
- Miglior supporto per il sistema di stampa Windows 200x/XP.
- Configurazione in qualità di server membro in domini Active-Directory.
- Assunzione di domini NT4 per poter effettuare la migrazione verso un dominio Samba.

Samba utilizza il protocollo SMB (Server Message Block), che si basa sui servizi di NetBIOS . Cedendo alle richieste della IBM, la Microsoft ha pubblicato il protocollo in modo da permettere anche ad altri fornitori di software di trovare il modo di 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.

Nota

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`.

Nota

NetBIOS

NetBIOS è un'interfaccia software (API) progettata per la comunicazione tra client; viene messo a disposizione un *name service* ai fini della identificazione reciproca dei client. 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. L'implementazione avviene ad un livello molto vicino all'hardware di rete e si chiama NetBEUI . NetBEUI viene spesso chiamato NetBIOS . Altri protocolli di rete con cui è stata implementato NetBIOS sono IPX (NetBIOS tramite TCP/IP) di Novell e TCP/IP.

I nomi NetBIOS che vengono anche assegnati all'implementazione di NetBIOS tramite TCP/IP non hanno niente a che vedere con i nomi assegnati nel file `/etc/hosts` o via DNS - NetBIOS dispone di un proprio name space. Per semplificare l'amministrazione è però consigliabile assegnare, almeno ai server, dei nomi NetBIOS che corrispondano al nome host DNS; per un server Samba ciò avviene di default.

Client

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 il file system adatto a SMB che permette di integrare risorse SMB a livello del 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 deve corrispondere al nome della directory esportata. Allo stesso modo viene attribuito un nome ad una stampante esportata, attraverso il quale i client possono indirizzarla.

17.1.2 Installazione e 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 viene chiamata `[share]`. Qui vengono definite le singole share per file e stampante. In tal modo, i dettagli riguardanti la share possono essere impostati singolarmente, oppure uniformemente nella sezione `[global]`. Ciò risulta in una maggior chiarezza per quanto riguarda i file di configurazione.

Sezione global in una configurazione esempio

I seguenti parametri della sezione `global` devono essere adattati alle caratteristiche della vostra rete, affinché il vostro server Samba sia indirizzabile tramite SMB per gli altri sistemi in una rete Windows.

workgroup = TUX-NET Con questa istruzione assegnate il server Samba ad un gruppo di lavoro. Adattate `TUX-NET` al gruppo di lavoro effettivamente esistente o configurate i client secondo i valori qui selezionati. 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` può essere impostato un nome che differisce dal nome DNS. Per maggiori dettagli su questo parametro 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 *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 ancora non gira un server SMB — p.es. Windows NT, 2000 Server — ed il server Samba dovrà mettere a disposizione nella rete locale i nomi dei sistemi disponibili, aumentate il valore dell'`os level` (a p.es. 65), per fargli assumere il ruolo di LMB.

Siate cauti nel modificare questo valore, poiché potreste causare dei disturbi 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 wins server Volete integrare un server Samba in una rete Windows esistente, con un server WINS in esecuzione: per fare questo dovete attivare il parametro `wins server` impostando questo parametro sull'indirizzo IP del server WINS.

Se i vostri sistemi Windows sono in esecuzione in sottoreti separate e devono essere visibili tra di loro vi serve 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 entrambi le opzioni `wins server` e `wins support` nel file di configurazione (smb.conf.)

Le share

Nei seguenti esempi vengono condivisi con client SMB il lettore di CD-ROM e le directory degli utenti, le `homes`.

`[cdrom]` Per evitare di sharare inavvertitamente un lettore di CD-ROM, tutte le righe necessarie alla share sono disattivate (punto e virgola). Se volete che il lettore di CD-ROM venga condiviso tramite Samba, cancellate il punto e virgola(';') a inizio riga.

Exempio 17.1: *Sharare il lettore di CD-ROM*

```
;[cdrom]
;       comment = Linux CD-ROM
;       path = /media/cdrom
;       locking = No
```

`[cdrom]` **e** `comment [cdrom]` è il nome share visibile ai client SMB. Con `comment` si può dare un nome espressivo alla share.

`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 a tutti, bisogna aggiungere la riga `guest ok = Yes`. Visto che ognuno ha 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: se un utente sul server di file Linux ha un valido account ed una propria directory home, il suo client si può collegare immettendo un login e una password validi.

Exempio 17.2: *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 esplicita con il nome share dell' utente che si connette, viene generata dinamicamente una share in base alla 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, gli utenti consentiti si limitano al proprietario della directory utente. Questo è un modo per consentire l'accesso solo al proprietario.

`browseable = No` Con questa impostazione la share `[homes]` non è visibile nell'elenco delle share.

`read only = No` Di default, Samba non consente l' accesso in scrittura a share esportate, `read only = Yes`. Se un indirizzario deve poter essere accessibile in scrittura, impostate il valore `read only = No` che equivale a `writeable = Yes`.

`create mask = 0640` I sistemi Windows non conoscono il concetto dei permessi d'accesso Unix; non possono perciò indicare, alla creazione di un file quali permessi d'accesso essi abbiano. Il parametro `create mask` stabilisce con quali permessi di accesso debbano venire creati i file. Questo vale solo per share con 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.

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 la conosce, 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 può, in base al nome dell'utente, accordare l'accesso alle singoli share esportate.

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 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 del server via Share Level Security ed altre via User Level Security. Comunque su di un sistema potete avere un server Samba per ogni indirizzo IP configurato.

Per ulteriori informazioni rimandiamo al Samba-HOWTO-Collection. Se amministrate diversi server su di un sistema dovete considerare i parametri `interfaces` e `bind interfaces only`.

Nota

Per una facile amministrazione del server Samba, vi inoltre il programma swat che mette a disposizione una semplice interfaccia web con la quale potete configurare comodamente il server Samba. Invocate in un browser `http://localhost:901` ed eseguite il login come root. Badate che swat è da abilitare anche nei file `/etc/xinetd.d/samba` e `/etc/services`, modificate a riguardo in `/etc/xinetd.d/samba` la seguente riga: `disable = no`. Per maggiori informazioni su swat consultate la pagina di manuale di swat.

Nota

17.1.3 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 con account e password validi. Questo può venire realizzato con l'aiuto di un server Samba. In una rete puramente Windows, un server Windows-NT si assume questo compito; esso è configurato come cosiddetto Primary Domain Controller (PDC). Nella sezione `[global]` di `smb.conf` dovrete impostare i seguenti parametri, come nell'esempio 17.3:

Exempio 17.3: *Sezione globale in smb.conf*

```
[global]
        workgroup = TUX-NET
        domain logons = Yes
        domain master = Yes
```

Se per la 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 `[globals]`, 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, questo viene creato con i seguenti comandi:

Exempio 17.4: *Creare un account macchina*

```
useradd nome-dell'-host\$
smbpasswd -a -m nome-dell'-host
```

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.

Exempio 17.5: *Creare automaticamente un account macchina*

```
add user script = /usr/sbin/useradd -g machines \
                  -c "NT Machine Account" -d \
                  /dev/null -s /bin/false %m\$
```

Affinché Samba esegua in modo corretto questo script è richiesto un utente Samba con i diritti di amministratore. Aggiungete per fare questo il gruppo `ntadmin` all'utente selezionato. In seguito potrete aggiungere tutti gli utenti di questo gruppo Unix ai "Domain Admins" tramite questo comando:

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

Per maggiori informazioni rimandiamo alla Samba-HOWTO-Collection del capitolo 12: `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

17.1.4 Installazione dei client

I client possono indirizzare il server Samba solo tramite TCP/IP. NetBEUI o NetBIOS via IPX non sono utilizzabili con Samba.

Windows 9x/ME

Windows 9x/ME supporta TCP/IP. Come per Windows per gruppi di lavoro (workgroup) tale supporto non viene però installato con l'installazione standard. Per installare successivamente TCP/IP, si seleziona nell'applet di ret delle risorse di sistema 'Aggiungere...' sotto 'Protocolli' TCP/IP di Microsoft. Dopo un reboot del computer Windows, ritroverete il server Samba con un doppio clic sul simbolo del desktop per l'ambiente di rete.

Nota

Per utilizzare una stampante dal server Samba si dovrebbe installare il driver di stampante PostScript generico 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.

Nota

17.1.5 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 sono reperibili nella pagina di manuale di `smb.conf` nella sezione `socket options` e nella pagina di manuale `socket(7)`. Per ulteriori informazioni consultate la `Samba-HOWTO-Collection` nel capitolo `Samba performance tuning`.

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 una configurazione pronta per quel che riguarda la rete e il nome del gruppo di lavoro. Nella configurazione esempio commentata in `examples/smb.conf.SuSE` trovate tante indicazioni utili per gli adattamenti alla vostre esigenze personali.

Nota

Il Samba-Team fornisce nella `Samba-HOWTO-Collection` una sezione dedicata al rilevamento di errori. Part V contiene inoltre delle istruzioni da seguire passo dopo passo per controllare la configurazione.

Nota

17.2 Netatalk

Con `netatalk`, potrete realizzare un performante server di file e di stampa per client Mac OS: potrete accedere ai dati di un computer Linux da un Macintosh oppure stampare per via di una stampante collegata.

`Netatalk` è una suite di programmi Unix che utilizzano il DDP (Datagram Delivery Protocol) implementato nel kernel e che implementano il gruppo di protocolli AppleTalk (ADSP, ATP, ASP, RTMP, NBP, ZIP, AEP e PAP).

Principalmente, Appletalk è un equivalente del più diffuso TCP (Transmission Control Protocol). Molti servizi basati su TCP/IP, p.e. per la risoluzione dei nomi host e la sincronizzazione dell'ora, trovano sotto AppleTalk il loro corrispondente. Al posto di ping (ICMP ECHO_REQUEST, Internet Control Message Protocol) viene usato il comando `aecho` (AEP, AppleTalk Echo Protocol).

Normalmente, sul server vengono avviati i seguenti tre demoni:

- atalkd("AppleTalk-Network-Manager"), che corrisponde approssimativamente al programma ip;
- afpd ("AppleTalk Filing Protocol daemon"), che mette a disposizione per i client Macintosh un'interfaccia per i file system di Unix;
- papd ("Printer Access Protocol daemon"), che permette di indirizzare stampanti nella rete (AppleTalk).

Potete esportare indirizzari del server - utile soprattutto in ambienti di rete eterogenee - e non solo tramite `Netatalk`, ma anche tramite Samba (per i client di Windows vd. il capitolo precedente) e NFS (vd. 14.9 a pagina 371). Back-up ed amministrazione dei permessi degli utenti possono essere gestiti centralmente dal server Linux.

Se utilizzate `Netatalk` dovete tenere presente le seguenti restrizioni:

- a causa della restrizione dei client Macintosh, le password degli utenti sul server possono essere lunghe al massimo 8 caratteri.
- i client Macintosh non possono accedere ai file di Unix con più di 31 caratteri
- i nomi dei file non possono contenere due punti (`:`) perché questi, in Mac OS, servono come separatori nei nomi dei percorsi.

17.2.1 Configurazione del server di file

Nella configurazione standard, per gli utenti registrati sul sistema Linux, `Netatalk` è già funzionante a pieno regime come server di file. Per poter usufruire delle sue proprietà, dovrete eseguire alcune impostazioni nei file di configurazione che troverete nell'indirizzario `/etc/netatalk/`.

Tutti i file di configurazione sono puri file di testo. Le righe con un # iniziale e le righe vuote vengono ignorate ("commenti"). Tramite il file `/etc/netatalk/netatalk.conf` vengono abilitati i diversi servizi (stampante, Appletalk Broadcast, Appletalk tramite TCP/IP, server dell'orario):

```
ATALKD_RUN=yes
PAPD_RUN=yes
AFPD_RUN=yes
TIMELORD_RUN=no
```

Configurare la rete – atalkd.conf

In `/etc/atalk/atalkd.conf` viene definito tramite quali interfacce sono disponibili determinati servizi. Nella maggior parte dei casi, si tratta di `eth0`, ed di solito è sufficiente se `eth0` è il solo lo valore ad essere immesso (come nel file-esempio). Immettete qui altre interfacce, nel caso usaste contemporaneamente più schede di rete. Se viene inizializzato il server, questi cerca nella rete le zone ed i server già esistenti e modifica le righe corrispondenti, registrando gli indirizzi della rete AppleTalk configurati. In questo caso, alla fine del file, troverete la seguente riga:

```
eth0 -phase 2 -net 0-65534 -addr 65280.57
```

Se volete eseguire configurazioni più complesse, troverete degli esempi nel file di configurazione. Per le altre opzioni, consultate la pagina di manuale di afpd.

Definire il server di file – afpd.conf

Il file `afpd.conf` definisce come debba apparire il vostro server di file su computer Mac-OS nel menù 'Scelta'. Alla stregua degli altri file di configurazione, anche questo file contiene dei commenti dettagliati che spiegano le varie opzioni.

Se qui non eseguite alcuna modifica, viene avviato solo il server di default e mostrato sotto 'Scelta' con il nome host. Quindi qui non dovete immettere

per forza qualcosa, comunque avete modo di definire i server di file con diversi nomi ed opzioni, per offrire p.e. uno speciale "server guest", sul quale è possibile archiviare file come "ospite":

```
"Guest server" -uamlist uams_guest.so
```

Oppure potete definire un server non accessibile per ospiti, ma solo agli utenti esistenti sul sistema Linux:

```
"Font server" -uamlist uams_clrtxt.so,uams_dhx.so
```

Questo comportamento viene regolato dall'opzione `uamlist`, a cui segue una lista dei moduli di autenticazione da usare, separati da virgole. Di default, tutti i procedimenti sono attivi.

Come standard, un server AppleShare mette a disposizione i suoi servizi non solo tramite AppleTalk, ma anche ("incapsulati") tramite TCP/IP. La porta di default è 548. Per ulteriori server AppleShare (sullo stesso host) che debbanno girare per via TCP, dovete allocare loro porte dedicate. Mettere a disposizione un servizio tramite TCP/IP permette di accedere al server anche tramite reti non-AppleTalk, come ad esempio l'Internet.

La sintassi sarebbe:

```
"Font server" -uamlist uams_clrtxt.so,uams_dhx.so -port 12000
```

Il server AppleShare appare poi nella rete con il nome `Font Server`, non permette alcun accesso agli "ospiti" ed è impostato sulla porta 12000. In questo modo è raggiungibile anche tramite router TCP/IPD.

Nel file `AppleVolumes.default` (che illustreremo dettagliatamente più avanti) viene stabilito quali directory (residenti sul server) del rispettivo server AppleShare vengano messe a disposizione come *volumi* di rete (ovvero directory accessibili tramite rete). Con l'opzione `-defaultvol` è possibile stabilire, per un server AppleShare, anche un altro file nel quale vengono eseguite impostazioni divergenti, p.e. (in una riga):

```
"Guest server"  -uamlist  uams_guest.so -defaultvol
/etc/atalk/AppleVolumes.guest
```

Altre opzioni sono spiegate nel file `afpd.conf`.

Directory e permessi di accesso – AppleVolumes.default

Nel file `AppleVolumes.default` definite le directory da esportare. I permessi di accesso vengono stabiliti per mezzo dei consueti permessi Unix validi peri utenti e gruppi.

Nota

In parte, qui la sintassi è cambiata: tenetelo presente quando fate l'update da una versione più vecchia a quella attuale; p.e. ora, al posto di `access=`, si ha `allow:` (un sintomo caratteristico sarebbe se sotto AppleTalk su client Mac si ha la visualizzazione delle opzioni al posto della indicazione del drive). Poiché ad un update vengono creati nuovi file con l'estensione `.rpmnew`, può darsi che, a causa della sintassi modificata, le vostre vecchie impostazioni non funzionino più.
Vi consigliamo di eseguire un back-up dei vostri file di configurazione, di assumere le vostre vecchie impostazioni nei nuovi file e di rinominare quindi i nuovi file. In questo modo, approfittate anche degli attuali e dettagliati commenti contenuti nel file di configurazione.

Nota

Accanto a `AppleVolumes.default`, possono venire creati altri file come ad esempio. `AppleVolumes.guest`, che vengono utilizzati da determinati server (con l'uso dell'opzione `-defaultvol` nel file `afpd.conf`; vd. sezione precedente).

La sintassi è molto semplice:

```
/usr/local/psfonts "PostScript Fonts"
```

significa che la directory Linux `/usr/local/psfonts/`, che si trova nella directory root, viene resa disponibile come volume AppleShare con il nome "PostScript Fonts".

Le opzioni vengono aggiunte alla riga, separate da uno spazio vuoto. Un'opzione molto utile è quella per la restrizione dei permessi di accesso:

```
/usr/local/psfonts "PostScript Fonts" allow:User1,@gruppo0
```

limita l'accesso al volume "PostScript Fonts" all'utente `User1` e ai componenti del gruppo `gruppo0`: naturalmente, questi devono essere noti al server. Allo stesso modo, potete escludere esplicitamente determinati utenti ad esempio con `deny:User2`

Ricordate che queste limitazioni valgono per l'accesso tramite AppleTalk e non hanno niente a che fare con i permessi dell'utente, se dispone del permesso di eseguire il login sul server stesso.

Per la raffigurazione delle resource-fork di file tipiche per Mac OS in un file system Linux, `Netatalk` crea delle directory `.AppleDouble`. Con l'opzione `noadouble` potete stabilire che queste directory vengano create solo quando sono effettivamente necessarie. Sintassi:

```
/usr/local/guests "Guests" options:noadouble
```

Per ulteriori opzioni e possibilità a vostra disposizione rimandiamo alle spiegazioni contenute nel file stesso.

Inoltre: in questo file di configurazione trovate anche una tilde (`'~'`). Questa tilde rappresenta la directory home di ogni utente sul server. In questo modo, si può mettere automaticamente a disposizione di ogni utente la sua directory home, senza doverla indicare esplicitamente. Il file- esempio installato contiene già una tilde e, se non modificate il file, `Netatalk` mette a disposizione le directory home.

Nella home directory di ogni utente registrato, afpd cerca un file `Applevolumes` o `.Applevolumes`. Le registrazioni di questi file completano quelle nei file di server `AppleVolumes.system` e `AppleVolumes.default`, per rendere possibili ulteriori correlazioni personalizzate type/creator e per accedere ai file system. Grazie a queste impostazioni viene impedito che un utente accedi in modo non autorizzato al server.

Il file `netatalk.pamd` serve all'autenticazione tramite PAM (Pluggable AuthenticationModules), ma non approfondiremo questo tema in questo capitolo.

Attribuzioni di file– AppleVolumes.system

Nel file `AppleVolumes.System` stabilite quali correlazioni type/creator (tipiche di Mac OS) devono seguire a determinate estensioni di file: sono già definiti una serie di valori standard. Se un file viene indicato con un'icona bianca generica, significa che non esiste ancora alcuna impostazione. Se doveste aver problemi ad aprire, sotto Mac OS, un file di testo di un altro sistema (o viceversa), controllate le impostazioni qui contenute.

17.2.2 Configurazione del server di stampa

Tramite il file `papd.conf` viene messo a disposizione un servizio laserwriter. La stampante `lpd` deve già funzionare localmente (si veda il

capitolo 5 a pagina 93). Se potete stampare localmente con il comando `lpr file.txt` avete già realizzato un importante primo passo.

Se, su Linux, è configurata una stampante locale, non dovete immettere niente in `papd.conf`, poichè, senza ulteriori indicazioni, gli incarichi di stampa vengono semplicemente inoltrati al demone di stampa `lpd`. La stampante appare nella rete AppleTalk come laserwriter. Potete però anche immettere una determinata stampante nel file di configurazione:

```
Stampante_ricezione:pr=lp:pd=/etc/netatalk/kyocera.ppd
```

Questi parametri fanno apparire, nella selezione, la stampante con il nome `Stampante_ricezione`. Il corrispondente file di descrizione della stampante lo potete di solito richiedere al produttore. Oppure, prendete il file `Laserwriter` dalla directory `Estensionidelsistema/`; in questo modo, però, spesso non potete usufruire di tutte le proprietà della stampante.

17.2.3 Inizializzare il server

Il server stesso viene inizializzato grazie agli `init-script`, ovvero script di inizializzazione, all' avvio del sistema o manualmente con il comando `rcatalk start`. Lo script di inizializzazione si trova in `/etc/init.d/atalk`. Il server viene avviato dallo script in background; occorre circa un minuto, prima che le interfacce AppleTalk siano configurate ed accessibili. Con una richiesta di stato potrete verificare se il processo è terminato (lo riconoscerete da un triplo `OK`):

```
rcatalk status

Checking for service atalk:OKOKOK
```

Passate ora ad un Mac che giri su Mac OS. Controllate che AppleTalk sia attivato, selezionate 'Filesharing', eseguite un doppio clic su 'Appleshare'; nella finestra dovreste ora vedere il nome del vostro server. Eseguitevi un doppio clic e fate il login. Selezionate il drive e ... voilà, ecco il vostro drive di rete su Mac OS.

Potete collegarvi con i server che funzionano solo con TCP e non con DDP, cliccando nella 'Scelta' su 'Indirizzo IP del server' ed immettendo l'indirizzo IP corrispondente, eventualmente seguito da due punti e il numero di porta.

17.2.4 Ulteriori informazioni

Per sfruttare a pieno tutte le possibilità offerte da `netatalk`, vi consigliamo di leggere le pagine di manuale corrispondenti. Come sempre, le troverete con il comando: `rpm -qd netatalk`. Ancora un'indicazione: il file `/etc/atalk/netatalk.conf` non è necessario nella nostra versione di netatalk: ignoratelo. URL di appoggio:

- `http://netatalk.sourceforge.net/`
- `http://www.umich.edu/~rsug/netatalk/`
- `http://www.anders.com/projects/netatalk/`

17.3 Emulazione Netware con MARSNWE

Con l'emulatore di Netware MARSNWE si può sostituire in modo relativamente facile un server Novell-NetWare 2.2 o 3.11 per servizi di file e stampa e si può usarlo nel contempo come router IPX. Tuttavia, l'emulatore non offre le funzionalità delle più recenti versioni di NetWare, come ad esempio, NDS *Netware Directory Services* . Apportando delle minime modifiche a delle postazioni di lavoro su cui gira DOS o Windows con accesso ad un server NetWare 2.2/3.11/3.12 si può fare in modo che le postazioni facciano capo ad un server Linux con l'emulatore di NetWare MARSNWE. L'amministrazione si realizza sotto Linux.

17.3.1 Lanciare l'emulatore NetWare MARSNWE

Il MARSNWE su SuSE Linux può essere lanciato subito dopo l'installazione, dal momento che é preconfigurato in modo da poter essere subito utilizzato. Il necessario supporto IPX del kernel è un modulo kernel caricabile che viene caricato automaticamente dallo script di inizializzazione all'occorrenza. Le interfacce IPX vengono configurate automaticamente da MARSNWE. Il numero di rete ed il protocollo da utilizzare sono reperibili nel file di configurazione ampiamente commentato `/etc/nwserv.conf`. Inizializzate MARSNWE con il comando `rcnwe start`. Se appare `done` in verde sulla destra dello schermo, vuol dire che il programma è stato avviato con successo.

Con `rcnwe`, verificate se l'emulatore è in esecuzione. Con `rcnwe status` lo fermate.

17.3.2 Il file di configurazione /etc/nwserv.conf

Le opzioni di configurazione sono riassunte in "section" numerate. Ogni riga di configurazione inizia sempre con il numero della sezione corrispondente. A noi interessano solo le sezioni da 1a 22, anche se non si utilizzano tutti i numeri. Normalmente, per la configurazione, bastano le sezioni seguenti:

1 Volumi Netware

2 Nome server

4 Rete IPX

13 User name

21 Stampante

Dopo ogni modifica apportata alla configurazione, rilanciate MARSNWE con il comando `rcnwe restart`.

Ed ecco le opzioni di configurazione in dettaglio:

Volumi (Section 1):
```
1     SYS     /usr/local/nwe/SYS/    kt     711 600
```

con cui vengono definiti i volumi da esportare. Ogni riga inizia con il numero della sezione (1, in questo caso), a cui segue il nome del volume e il percorso della directory sul server. Possono essere indicate ancora tutta una serie di opzioni, rappresentate da lettere singole, nonché una UMASK per la creazione di indirizzari e una per file. In assenza di UMASK, viene usato il valore standard della section 9. Il volume per SYS è già riportato. Per evitare problemi con maiuscole e minuscole, si consiglia di usare l'opzione `k`, che converte i nomi dei file in minuscole.

Nome server (Section 2):
```
2     MARS
```

facoltativo: normalmente, viene usato il nome dell'host.

Numero di rete interno (Section 3):
```
3     auto
```

`auto` vuol dire che il numero di rete interno viene generato dall'indirizzo MAC della scheda di rete. Questa impostazione viene normalmente mantenuta.

Configurazione IPX (Section 4):

```
4    0x0     *       AUTO            1
4    0x22    eth0    ethernet_ii     1
```

Qui si indica il numero di rete Netware e su quale interfaccia di rete debba essere collegata tramite quale protocollo. Il primo esempio imposta tutto in automatico, mentre il secondo collega il numero di rete `0x22` sulla scheda di rete `eth0` con il tipo di frame `Ethernet-II`. Se si hanno di più schede di rete e le si registra con numeri di rete diversi, IPX svolge il routing.

Create Mode (Section 9):

```
9    0751    0640
```

Indica i permessi standard con i quali vengono creati directory e file.

GID e UID con diritti minimi (section 10, 11):

```
10   65534
11   65534
```

ID di gruppo e d'utente per utenti non registrati. In questo caso: `nogroup` e `nobody`.

Supervisor Login (Section 12):

```
12   SUPERVISOR      root
```

Il supervisor viene rappresentato dall'utente `root`.

Login dell'utente (Section 13):

```
13   LINUX           linux
```

Qui si stabilisce la correlazione tra utenti Netware ed utenti Linux. Avete l'opzione di indicare una password fissa.

Rappresentazione automatica degli utenti (Section 15):

```
15   0               top-secret
```

Se si ha `1` invece di `0`, i login di Linux diventano automaticamente disponibili come login di Netware. La password, in questo esempio, è "top-secret".

Coda di stampa (Section 21):

```
21   LP              lpr -
```

Il primo parametro `LP` è il nome della stampante Netware. Al secondo posto, potete immettere il nome della directory spool e, al terzo, il comando di stampa.

Server di stampa (Section 22):

```
22   PS_NWE  LP_PS   1
```

Definizione delle stampanti indirizzabili tramite il programma pserver di `ncpfs`.

17.3.3 Accesso ai server Netware e la loro amministrazione

Il `ncpfs` è una raccolta di piccoli programmi che permettono di amministrare i server Netware 2.2/3.11 da Linux, di montare volumi Netware o amministrare le stampanti. Per accedere a server Netware più recenti, dalla versione 4 in poi, bisogna che vi siano attivati l'emulazione Bindery e l'IPX.

A questo scopo servono i seguenti programmi, le cui funzioni sono riportate e documentate nelle relative pagine di manuale:

nwmsg	ncopy	ncpmount	ncpumount
nprint	nsend	nwauth	nwbocreate
nwbols	nwboprops	nwborm	nwbpadd
nwbpcreate	nwbprm	nwbpset	nwbpvalues
nwdir	nwdpvalues	nwfsctrl	nwfsinfo
nwfstime	nwgrant	nwpasswd	nwpurge
nwrevoke	nwrights	nwsfind	nwtrustee
nwtrustee2	nwuserlist	nwvolinfo	pqlist
pqrm	pqstat	pserver	slist

Importante è, p.e., `ncpmount`, che serve a montare i volumi di un server NetWare sotto Linux, e `ncpumount` , per eseguire il processo inverso ovvero 'smontarli'.

Inoltre, il pacchetto `ncpfs` contiene strumenti per la configurazione del protocollo IPX e del routing IPX:

```
ipx_cmd
ipx_configure
ipx_interface
ipx_internal_net
ipx_route
```

`ipx_configure` o `ipx_interface` servono a configurare l'IPX della scheda di rete; se MARSNWE è in esecuzione, ciò viene fatto automaticamente.

17.3.4 Router IPX con ipxrip

Per trasformare Linux in un router IPX, vi è inoltre il pacchetto `ipxrip`. Di solito non se ne ha bisogno, dal momento che è possibile configurare un router IPX anche con MARSNWE o grazie agli strumenti di ncpfs.

Internet

L' Internet si è oramai affermato come piattaforma di comunicazione; Linux quale sistema operativo di rete è in grado di assolvere a una serie di compiti sia in funzione di server che di client. In questo capitolo tratteremo alcuni temi di sicuro interesse: l'assistente di dial-in smpppd (SUSE Meta PPP Daemon), la configurazione manuale di un accesso ADSL, per il caso che si dovessero verificare delle difficoltà durante la configurazione con YaST e la configurazione del proxy Squid.

18.1 smpppd come assistente di selezione

18.1.1 Componenti di programma per entrare in Internet

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 si ha una flat-rate (canone fisso) senza che vengano addebbitati dei costi aggiuntivi per stabilire la connessione, è sufficiente che si avvia correttamente il demone (deamon). Spesso comunque si desidera controllare il collegamento tramite un applet di KDE ovvero un miniprogramma di KDE oppure tramite un'interfaccia per la riga di comando. Inoltre spesso l'internet gateway è un altro computer rispetto alla postazione di lavoro effettivamente utilizzata, e così spesso ci si ritrova a dover monitorare il collegamento ad Internet realizzato tramite un computer indirizzabile via rete.

Ed è qui che entra in gioco smpppd (SUSE 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. Dall'altra 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.

18.1.2 Configurare smpppd

La configurazione della connessione che smpppd mette a disposizione viene svolta automaticamente da YaST. I programmi con cui si entra effettivamente in Internet come kinternet e cinternet vengono anche loro 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 qui si può stabilire tramite quale indirizzo IP smpppd accetta delle connessioni.

host-range = <min ip> <max ip>
Il parametro `host-range` definisce un'area di rete. I computer con un indirizzo IP all'interno di questo intervallo hanno il permesso di accedere a smpppd e a tutti i computer che non si trovano in questa area l'accesso viene negato.

password = <password> Con l'impostazione di una password si restringere l'accesso dei client ai soli computer con autorizzazione. Visto che comunque si tratta di una password non cifrata, non sopravvalutate l'aspetto in termini sicurezza di questa impostazione. Se non si imposta alcuna password tutti i client hanno l'autorizzazione di accedere a smpppd.

Per ulteriori informazioni su smpppd consultate le pagine di manuale `man smpppd` e `man smpppd.conf`.

18.1.3 Preparare kinternet e cinternet per l'utilizzo in remoto

kinternet e cinternet possono essere sia utilizzati in locale che per controllare un smpppd remoto. cinternet è la variante testuale che si basa sulla riga di comando di kinternet con interfaccia grafica. Se volete preparare queste utility per l' uso assieme a uno smpppd remoto, dovrete editare il file di configurazione `/etc/smpppd-c.conf` manualmente o tramite kinternet. Questo file conosce solo tre opzioni:

server = <server> Qui potete specificare l'host su cui gira smpppd. Se si tratta contemporaneamente del gateway di default del computer, è sufficiente impostare `gateway-fallback` su `yes`.

gateway-fallback = <yes|no> Se non è stato specificato alcun server né vi è uno in esecuzione localmente, si può tentare di indirizzare un smpppd sul gateway di default. Questa opzione è abilitata di default.

password = `<password>` Immettete qui la password pensata anche per smpppd.

Se smpppd è in esecuzione potete provare ad accedervi. Si consiglia di utilizzare in questi casi il comando `cinternet --verbose --interface-list`. Per maggiori dettagli consultate le pagine di manuale `man smpppd-c.conf` e `man cinternet`.

18.2 Configurazione di un collegamento DSL/ADSL

18.2.1 Configurazione standard

Al momento, SuSE Linux supporta accessi DSL che si basano sul protocollo Point-to-Point-over-Ethernet (PPPoE). Questo protocollo viene impiegato dai maggiori provider. Se non siete sicuri riguardo al protocollo utilizzato dal vostro provider, chiedeteglielo.

1. I pacchetti `ppppp` `smpppd` e devono essere installati. Il modo migliore di installarli è quello di usare YaST.
2. Configurate la vostra scheda di rete con YaST. Non usate `dhcp`, ma assegnatele un indirizzo IP statico, ad esempio, `192.168.2.22`.
3. I parametri che modificherete con il modulo YaST DSL vengono salvati nel file `/etc/sysconfig/network/providers/dsl-provider0`. Vi sono anche file di configurazione per smpppd (SuSE meta-ppp-deamon) ed i suoi front-end kinternet e cinternet. Vd. la pagina di manuale `smpppd` .
4. Avviate la rete anche con il comando `rcnetwork start` ed in seguito l' smpppd con `rcsmpppd start`.
5. Con i comandi `cinternet --start` e `cinternet --stop`, potete aprire e chiudere una connessione su di un sistema senza interfaccia grafica. Con un'interfaccia grafica, potete utilizzare anche kinternet, che viene avviato automaticamente se avete configurato DSL con YaST: cliccate sulla ruota dentata nella barra dei bottoni e selezionate 'Comunicazione/Internet'→'Internet Tools'→'kinternet'. Nella barra dei bottoni apparirà ora uno spinotto: cliccateci sopra per connettervi e ricliccateci per chiudere la connessione.

18.2.2 Collegamento DSL Dial-on-Demand

Dial-on-Demand significa che il collegamento avviene automaticamente non appena l'utente vuole navigare su Internet, ad esempio, selezionando una pagina web tramite browser o spedendo un'e-mail. Se, per un determinato periodo di tempo (idle time), non vengono né inviati né ricevuti dati, il collegamento viene interrotto. Poiché PPPoE, il protocollo per ADSL, è molto veloce, si ha l'impressione di avere una connessione fissa.

- La maggioranza dei provider interrompe il collegamento dopo un determinato lasso di tempo.
- Un collegamento permanente può essere visto come uno spreco di risorse (ad esempio, di indirizzi IP)
- Essere perennemente connessi ad Internet comporta dei rischi, dal momento che qualcuno potrebbe tentare di individuare dei punti deboli del vostro sistema. Una connessione puntuale con indirizzi IP sempre diversi è molto più difficile da attaccare.

Potete abilitare il Dial-on-Demand con YaST (vd. anche il manuale dell'utente) o manualmente. Nel file `/etc/sysconfig/network/providers/provider0`, impostate il parametro `DEMAND=` su yes e definite un idle time ovvero tempo di attesa con la variabile `IDLETIME="60"`(che interrompe una connessione inattiva dopo 60 secondi).

Ai fini della configurazione di un gateway DSL per reti private consigliamo di leggere il seguente articolo della nostra banca dati di supporto: `http://sdb.suse.de/en/sdb/html/masq80.html`(in inglese)

18.3 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 si ottengono statistiche sul carico della cache con l'aiuto di programmi come Calamaris e cachemgr o come filtrare contenuti web con squidGuard.

18.3.1 Cos'è una cache-proxy?

Squid funge da cache di proxy. Si comporta come un intermediario che riceve richieste da client (in questo caso il browser web) e le inoltra al server competente. Quando gli oggetti richiesti arrivano all'intermediario, questi ne ritiene una copia nella cache del disco rigido.

Il vantaggio è che quando più client richiedono lo stesso oggetto potranno ora venire serviti direttamente dalla cache del disco rigido, molto più velocemente che da Internet. Ciò risparmia molta banda del sistema.

Nota

Squid offre un vasto spettro di proprietà; p.e. la definizione di gerarchie per il server proxy per la distribuzione dei carichi del sistema, designazione di regole di accesso fisse per tutti i client che vogliono accedere al proxy, assegnare o negare dei permessi di accesso a determinate pagine web con l'aiuto di altre applicazioni o l'emissione di statistiche delle pagine web maggiormente visitate (p.e. il comportamento di navigazione degli utenti in Internet, e tanto altro ancora.)

Nota

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 supportate diversi programmi multi-media.

18.3.2 Informazioni sulla cache proxy

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: qui è importante che tutti i computer nella DMZ mandino i loro file di protocollo ai computer che si trovano all'interno della rete protetta.

Una possibilità di implementare un proxy cosiddetto "trasparente" viene trattata nella sezione 18.3.6 a pagina 471.

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 scaricare (download) 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.e. 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 *Internet Cache Protocol*, che è basato sul protocollo UDP. Lo scambio di dati fra le cache avviene tramite HTTP *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.

Nota

Per evitare la memorizzazione molteplice di oggetti in diverse cache della nostra rete, vengono usati altri protocolli ICP come p.e. CARP *Cache Array Routing Protocol* o HTCP *Hyper-Text Cache Protocol*. Più oggetti si trovano nella nostra rete, più grande sarà la possibilità di trovare quello cercato.

Nota

La memorizzazione temporanea 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.e. 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 *Last Recently Used* che sono stati concepiti per sostituire oggetti della cache. Il principio è quello di sostituire come primo gli oggetti meno richiesti.

18.3.3 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 sopravvalutare queste esigenze, 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.

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 in millesimi di secondo come "tempo casuale di posizionamento". Una regola approssimativa: più basso è questo valore e meglio è.

Un altro espediente per aumentare la velocità di trasmissione dei dati consiste nell'usare contemporaneamente più dischi rigidi o Raid Array stripe.

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 GB` e gli utenti necessitano di `10 MB` 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/sec` il tasso di trasmissione massimo è di `125 KB/sec`. Se il traffico completo dei dati arriva nella cache, entro un'ora avremo un totale di `450 MB`. Partendo dal presupposto che il completo traffico dei dati si svolga entro 8 ore di lavoro, in un giorno avremo "raccimolato" `3,6 GB`. Poiché di solito il collegamento non viene stato sfruttato fino in fondo, possiamo partire dal presupposto che la quantità di dati che passa attraverso la nostra cache, sia di ca. `2 GB`. Nel nostro esempio, abbiamo bisogno di `2 GB` di memoria per Squid, allo scopo di tenere nella cache i dati di tutte le pagine visitate durante *un* giorno.

Ricapitolando, possiamo dire che Squid tende a leggere o archiviare blocchi di dati più piccoli dal disco rigido, di modo che è più importante il tempo che il disco rigido impiega a trovare questi oggetti, che possedere un disco con un elevato numero di giri con un posizionamento rapido della testina.

RAM

La memoria 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 di un disco rigido!

Squid mantiene nella memoria anche molti altri dati, come p.e. una tabella con tutti gli indirizzi IP assegnati, una ben determinata cache per nomi di domini, gli oggetti più richiesti, buffer, ACL, etc.

È 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 18.3.7 a pagina 474.

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.

Sotto `http://www.cache.ja.net/servers/squids.html` troverete alcuni esempi di sistemi configurati sui quali gira Squid.

18.3.4 Avviare Squid

Lo Squid su SUSE LINUX è già preconfigurato e può essere subito 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`.

Per avviare Squid inserite (come `root`) nella riga di comando:`rcsquid start` . Al primissimo avvio, viene prima creata la struttura della directory in `/var/squid/cache`; ciò viene automaticamente eseguito dallo script di avvio `/etc/init.d/squid` e può durare un paio di secondi. Se sulla destra, in verde apparirà*done*, significa che Squid è stato avviato con successo. Sul sistema locale è possibile collaudare subito la funzionalità di Squid, immettendo nel browser come proxy `localhost` e `Port 3128`. 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, vd. il paragrafo 18.3.5 a pagina 468.

Se si sono eseguite delle modifiche nel file di configurazione `/etc/squid.conf`, bisogna indurre Squid a ricaricarlo. Questo avviene con: `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.

Attenzione

Terminare Squid

Se chiudete Squid con un `kill` o `killall`, ciò può causare la distruzione della cache. Per riavviare Squid dovreste cancellarla completamente.

Attenzione

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 YaST bisogna attivare Squid per determinati runlevel.

Se disinstallate Squid, la cache e i file di log rimangono; dunque, si dovrà cancellare manualmente la directory `/var/squid`.

Server DNS locale

Vale la pena configurare un server DNS locale come `BIND-9` , anche se non si amministra alcun dominio: funge solo da "DNS caching-only" ed è anche in grado di risolvere, tramite il server dei nomi root, richieste DNS senza aver bisogno di una configurazione speciale. Se lo si registra nel `/etc/resolv.conf` con l'indirizzo IP `127.0.0.1` per `localhost`, all'avvio Squid trova sempre un server dei nomi valido. Basta installare il pacchetto e lanciare BIND. Il server dei nomi del provider deve venire registrato nel file di configurazione `/etc/named.conf` sotto `forwarders` . Se avete un firewall in funzione, anche se si tratta solo di un personal firewall, si deve fare attenzione che vengano fatte passare le richieste DNS.

18.3.5 Il file di configurazione /etc/squid.conf

Tutte le impostazioni del server proxy Squid devono venire eseguite nel file `/etc/squid.conf`; per poter inizializzare Squid per la primissima volta, non è necessario eseguirvi alcuna modifica, ma, in un primo momento, è disdetto 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 molti 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. È sempre meglio lasciare invariato l'esempio ed inserire l'opzione con il parametro modificato nella riga inferiore. In questo modo, si vedono i valori preimpostati e le modifiche.

Nota

Update da versione 2.4 a versione 2.5

Dopo un aggiornamento di Squid dalla versione 2.4 alla versione 2.5 si deve cancellare la cache di Squid, dato che è cambiata la struttura delle directory.

Nota

Se avete aggiornato una vecchia versione di Squid, è assolutamente consigliabile usare il nuovo `/etc/squid.conf` e adottare solo le modifiche del file originale. Se cercate di continuare ad utilizzare il vecchio `squid.conf`, correte il pericolo che la nuova configurazione non funzioni più, poiché le opzioni vengono continuamente modificate e ne vengono aggiunte continuamente delle nuove.

Opzioni generali di configurazione

http_port 3128 La porta sulla quale Squid si mette "in ascolto" per richieste dei client. È preimpostata su `3128`, ma viene usata anche `8080`. Qui è possibile indicare più numeri di porte, divisi da uno spazio.

cache_peer <hostname> <type> <proxy-port> <icp-port>
Qui è possibile indicare un proxy superiore come "parent" (genitore), p.e. se si vuole o si deve usare il proxy del provider. Come <*hostname*> viene registrato il nome o l'indirizzo IP del proxy da usare e come <*type*> viene registrato *parent*. Per la <*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`. Se non è nota la porta ICP del parent e non se ne è concordato l'uso con il provider,l'<*icp-port*> può venire impostata su `7` o su `0`. 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 MB Questa registrazione indica il massimo di RAM usata da Squid per il caching. La preimpostazione è di `8 MB`.

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 `MB` 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 MB`

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 al massimo 80% dello spazio disponibile. È bene essere molto prudenti con l'aumento della quantità delle directory, poiché troppe directory possono causare problemi di prestazione. 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 file 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 chiama `squid -k rotate`, Squid è in grado di ruotare i file di log memorizzati: i file vengono numerati in relazione alla loro quantità e, dopo aver raggiunto il valore indicato, il file più vecchio viene sovrascritto. Di norma, questo valore è impostato su `0`, perché in SUSE LINUX l' archiviazione e l'eliminazione

dei file log vengono eseguite da un job di cron configurato nel file `/etc/logrotate/squid`.

append_domain <domain> 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. Se si ha però una linea commutata, può succedere che per un po' Internet risulti 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 modificare i *minutes* in *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 *all* per <*acl_name*>, tutte le richieste vengono inoltrate direttamente al *parent*. Ciò può essere necessario se p.e. si utilizza un provider che prescrive l'uso del suo proxy o se il firewall non consente alcun accesso diretto ad Internet.

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 effettivamente , p.e. assieme a *http_access*, vengono applicate le regole definite.

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.conf`. Cosa indicare per <*data*> dipende dal tipo di ACL e può provenire anche da un file, p.e. con 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* blocchino 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 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`. Cioè 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.e., 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.

authenticate_program /usr/sbin/pam_auth

Se si vuole che gli utenti si autenticano al proxy, si può indicare qui un programma adeguato, p.e.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' su tutti i client 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. Affinché 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.

18.3.6 Configurazione del proxy 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.
- È 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.

Configurazione del kernel

Prima assicuratevi che il kernel del server proxy supporti il proxing trasparente. Altrimenti dovete aggiungere questa opzione al kernel e ricompilarlo. Informazioni più precise a riguardo nel capitolo 11 a pagina 255. I moduli del kernel cambiano da versione a versione. Controllate lo stato attuale sotto `/usr/share/doc/howto/en/html/mini/TransparentProxy-3.html` o su Internet: `http://www.tldp.org/HOWTO/mini/TransparentProxy-3.html`.

Opzioni di configurazione in /etc/squid.conf

Nel file `/etc/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

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 proprio di SuSE: SuSEfirewall2, il cui file di configurazione si trova in `/etc/sysconfig/SuSEfirewall2`. Il file di configurazione è composto da registrazioni ben documentate. Anche se vogliamo configurare solo un proxy trasparente, dobbiamo configurare alcune opzioni inerenti al firewall, p.es.:

- Dispositivo punta su Internet: `FW_DEV_EXT`="eth1"
- Dispositivo punta sulla rete: `FW_DEV_INT` ="eth0"

Alle porte ed ai servizi (vd. `/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"

Alle porte ed ai servizi (vd. `/etc/services`) dietro il firewall accedono reti sicure, sia 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:

Exempio 18.1: *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 originale e
# 4) porta locale alla quale deve venire deviato il traffico,
# separato da virgole, p.e. "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. Prima accedono gli indirizzi IP e la scheda di rete delle "reti interne" al firewall di proxy: quindi gli indirizzi IP e le 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 deviare al proxy anche le richieste da altre porte, come FTP (porta 21), HTTPS o SSL (porta 443).

Concretamente, i servizi web (Port `80`) vengono deviati 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 18.3.4 a pagina 464. 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*⟩.

18.3.7 Squid ed altri programmi

In questa sezione vi mostriamo come interagiscono altre applicazioni con Squid. cachemgr.cgi consente all'amministratore di sistema di controllare lo spazio necessario per la memorizzazione temporanea di oggetti. Squidgrd filtra pagine web e calamaris genera dei resoconti per Squid.

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.

Configurare

Per prima cosa, è necessario sul sistema un server web funzionante. Per sapere se Apache è già in funzione, dobbiamo inserire come utente `root`: `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:

ACL del cache manager in /etc/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 ottenute 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 18.2 a fronte.

Exempio 18.2: *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 18.3.

Exempio 18.3: *Regole di accesso*

```
http_access allow manager localhost
http_access allow manager webserver
http_access deny manager
```

Se vogliamo accedere a più opzioni (p.e. 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`

Visualizzare le statistiche

Andate alla relativa pagina web, p.e.:`http://webserver.example.org/cgi-bin/cachemgr.cgi`. Premete su 'continua' 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.

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 i 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/conoscuiti per alcuni utenti.
- negare l'accesso ad alcuni utenti a determinati server web e/o URL.
- negare l'accesso ad URL ad utenti che usano 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.

L'uso di SquidGuard

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 intelligente 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" processi di reindirizzo, in questo caso squidGuard in esecuzione sul computer. 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 non consigliamo di stabilire più di 4 processi, poiché l'attribuzione di questi processi consuma inutilmente molta memoria.

```
redirect_children 4
```

Per concludere, fate caricare la nuova configurazione di Squid: `rcsquid reload`. Ora potete testare le vostre impostazioni su un browser.

Creare 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, fate 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 viene normalmente usata per l'emissione di tutti i rapporti disponibili con

-w si ottiene un rapporto HTML e con

-l una messaggio o un logo nell'intestazione del rapporto.

Nella pagina di manuale di calamaris, `man calamaris`, troverete altre informazioni sulle diverse opzioni.

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/`

18.3.8 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 proxy trasparente è nel `howtoen`, 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/`.

Sicurezza nella rete

Mascheramento, firewall e Kerberos formano le basi di una rete sicura con un traffico di dati monitorato. La secure shell (SSH) dà all'utente la possibilità di accedere ad un host remoto tramite una connessione cifrata. Per poter usufruire di tutte queste possibilità a vostra disposizione, tratteremo gli aspetti principali che riguardano la sicurezza della rete.

19.1 Masquerading e Firewall

Grazie alle sue spiccate capacità di rete, Linux viene sempre più spesso utilizzato come router per linee commutate e non. Qui la definizione router si riferisce ad un computer con più di un'interfaccia di rete ed in grado di inoltrare ai suoi rispettivi partner di comunicazione i pacchetti che non sono destinati ad una delle proprie interfacce di rete. Spesso un router viene anche chiamato gateway. Con i filtri dei pacchetti presenti nel kernel di Linux è possibile controllare esattamente quali pacchetti del traffico dati hanno il permesso passare e quali no.

Per determinare i precisi criteri di filtraggio di questo filtra pacchetti, l'amministratore dovrà disporre di una certa esperienza. Per gli utenti meno esperti, SUSE Linux contiene un pacchetto a sé stante `SuSEfirewall2` pensato per facilitare l'impostazione di questi criteri.

La configurazione di `SuSEfirewall2` è molto flessibile e perciò adatta anche alla creazione di costrutti più complessi per il filtraggio di pacchetti. Il pacchetto per il filtraggio dei pacchetti permette di impiegare un computer Linux - tramite masquerading - come router per creare una rete interna con un solo indirizzo IP visibile dall'esterno. Il mascheramento viene anche realizzato in base alle regole di un filtra pacchetti.

Attenzione

I procedimenti qui presentati sono standardizzati e generalmente funzionano: non possiamo tuttavia garantire che non si sia infiltrato un qualche erroretto in questo manuale o altrove. Se dei cracker riescono ad entrare nel vostro sistema, nonostante abbiate fatto tutto a puntino, non datene la colpa agli autori. Anche se non doveste ricevere una risposta diretta, siate pur certi che vi saremo grati per ogni vostra critica o suggerimento e provvederemo immediatamente a fare ammenda.

Attenzione

19.1.1 I principi del masquerading

Masquerading è l'adattamento Linux di NAT (*Network Address Translation*), cioè "traduzione di indirizzi rete". Il principio di NAT non è particolarmente complicato: il vostro router ha più di un'interfaccia di rete, normalmente una scheda di rete e una interfaccia a parte per l'Internet (p.e. un'interfaccia ISDN). Una di queste interfacce vi collegherà con l'esterno, una o più delle altre interfacce collegheranno il vostro computer con gli altri computer nella vostra rete. Facciamo ora un esempio e ci colleghiamo

via ISDN con l'esterno tramite l'interfaccia di rete `ippp0`. Nella vostra rete locale avete collegato più computer alla scheda di rete del router Linux la quale, nel nostro esempio, si chiamerà `eth0`. Gli host nella rete inviano i pacchetti destinati all'esterno al router o al gateway di default.

Nota

Quando configurate la vostra rete, fate attenzione alla conformità degli indirizzi broadcast e maschere di rete!

Nota

Se uno dei computer nella vostra rete invia ora un pacchetto su 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 non viene eseguito dall'installazione di SUSE LINUX! Impostate la variabile `IP_FORWARD` che si trova nel file `/etc/sysconfig/network/options` su `IP_FORWARD=yes`. Dopo il reboot o con il comando `echo 1 > /proc/sys/net/ipv4/ip_forward` viene attivato l'inoltro.

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.

I pacchetti, che fanno parte del collegamento, creati ricorrendo al mascheramento attraverso il router vengono riconosciuti grazie ad una tabella mantenuta direttamente nel kernel del vostro router per il periodo di tempo in cui i rispettivi collegamenti sono attivi: questa tabella può venire esaminata dal superutente (`root`) con il comando `iptables`. Per avere indicazioni più precise, consultate la pagine di manuale di questo comando. Per l'identificazione di singoli collegamenti mascherati, sono importanti, oltre all'indirizzo mittente e ricevente, anche il numero della porta ed i protocolli interessati. In questo modo, il vostro router è in grado di mettere a disposizione contemporaneamente numerosi collegamenti per ciascuno dei vostri host locali.

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 un stato ben definito, di modo che i relativi parametri nella tabella non possano venire utilizzati da un secondo collegamento.

Di conseguenza, subentrano difficoltà con alcune applicazioni: per esempio ICQ, cucme, IRC (DCC, CTCP), Quake 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.

19.1.2 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 monitorizzato. Esistono diversi tipi di firewall che si distinguono principalmente a livello logico-astratto della verifica e la regolamentazione del traffico dei dati. Per essere più precisi, il metodo che vi presentiamo qui dovrebbe chiamarsi filtra pacchetti. Un filtro pacchetti regola il transito sulla base di norme i cui criteri sono protocolli, porte ed indirizzi IP. In questo modo, siete in grado di intercettare quei pacchetti che, sulla base del loro indirizzo, non possono entrare nella vostra rete. È per esempio consigliabile intercettare quei pacchetti che utilizzano il servizio telnet destinati alla porta 23 del vostro computer. Se però volete permettere l'accesso al vostro server web, dovete attivare la porta corrispondente. Il contenuto di questi pacchetti non viene controllato finchè sono indirizzati in modo corretto (p.e. 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 per un application gateway. Questo gateway o 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 `howtoen`. Se questo pacchetto è stato installato, potete leggerlo con il comando `less /usr/share/doc/howto/en/Firewall-HOWTO.txt.gz`.

19.1.3 SuSEfirewall2

La configurazione del SuSEfirewall2 richiede già un certo bagaglio di esperienza. Sotto `/usr/share/doc/packages/SuSEfirewall2` trovate comunque la documentazione relativa al SuSEfirewall2.

Potrete eseguire la configurazione ricorrendo ad YaST (vd. la sezione 19.1.3 a pagina 485) o direttamente nel file `/etc/sysconfig/SuSEfirewall2` che contiene delle indicazioni in lingua inglese.

Configurazione manuale

Segue una guida passo per passo alla configurazione. In ogni punto, viene indicato se quanto detto vale per il masquerading o firewall. Nel file di configurazione si parla anche di una DMZ (Zona demilitarizzata); ma questo esula dalla nostre considerazioni.

Se avete veramente bisogno soltanto del mascheramento, compilate solo le righe contrassegnate con *Masquerading*.

- Inizializzate il SuSEfirewall2 per il vostro runlevel (probabilmente 3 o 5) con l' editor del runlevel di YaST. Così vengono creati dei link simbolici per gli script SuSEfirewall2_* nelle directory `/etc/init.d/rc?.d/`.
- `FW_DEV_WORLD` (Firewall, Masquerading): p.e. `eth0`, il dispositivo vi porta su Internet. Nel caso di ISDN è p.e. `ippp0`.
- `FW_DEV_INT` (Firewall, Masquerading): il device che punta alla rete interna, privata. Se non esiste alcuna rete interna lasciate vuota questa variabile.
- `FW_ROUTE` (Firewall, Masquerading): se vi serve il masquerading, impostate questa variabile su `yes`. I vostri computer interni non sono visibili dall'esterno, dal momento che hanno indirizzi di rete privati (p.e. `192.168.x.x`) che non verranno inoltrati (routed) su Internet.

  Per un firewall senza masquerading selezionate qui `yes`, solo se volete permettere l'accesso alla rete interna. Per fare questo i computer interni devono avere indirizzi IP assegnati ufficialmente. Di solito però, *non* dovreste consentire un accesso ai vostri computer dall'esterno!
- `FW_MASQUERADE` (Masquerading): se intendete fare uso del mascheramento, immettete qui `yes`. Tenete presente che è più sicuro se i computer della rete interna accedono ad Internet tramite il server proxy.

- `FW_MASQ_NETS` (Masquerading): 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. Vedi anche `FW_SERVICES_INTERNAL_TCP` e `FW_SERVICES_INTERNAL_UDP`.
- `FW_AUTOPROTECT_GLOBAL_SERVICES` (Firewall): lasciare di solito su `yes`.
- `FW_SERVICES_EXTERNAL_TCP` (Firewall): registrate qui i servizi a cui si deve accedere; p.e. `www smtp ftp domain 443` – per il computer casalingo che non deve offrire alcun servizio, non inserite niente.
- `FW_SERVICES_EXTERNAL_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 necessarie.
- `FW_SERVICES_INTERNAL_TCP` (Firewall): qui trovate i servizi disponibili per la rete interna. Le indicazioni sono analoghe a quelle in `FW_SERVICES_EXTERNAL_TCP`, si riferiscono però qui alla rete *interna*.
- `FW_SERVICES_INTERNAL_UDP` (Firewall): Vedi sopra.
- `FW_TRUSTED_NETS` (Firewall): qui registrate gli host di cui potete *veramente* fidarvi (trusted hosts). Tenete però a mente che anche questi host devono venire protetti contro intrusioni. Esempio: `172.20.0.0/16 172.30.4.2` significa che tutti gli host con indirizzi IP che iniziano con `172.20.x.x`, come pure l'host con l'indirizzo IP `172.30.4.2` sono abilitati a passare il firewall.
- `FW_SERVICES_TRUSTED_TCP` (Firewall): qui potete stabilire gli indirizzi di porta TCP, che possono venire usati dai Trusted Hosts. Registrate p.e. `1:65535` se i computer affidabili possono accedere a tutti i servizi. Normalmente, dovrebbe essere sufficiente immettere qui `ssh` come servizio.
- `FW_SERVICES_TRUSTED_UDP` (Firewall): come sopra, solo riferito a UDP.

- FW_ALLOW_INCOMING_HIGHPORTS_TCP (Firewall): se volete utilizzare un normale FTP (attivo), digitate qui ftp-data.
- FW_ALLOW_INCOMING_HIGHPORTS_UDP (Firewall): inserite dns per poter usare i server dei nomi registrati in /etc/resolv.conf. Con yes attivate tutte le porte con numeri alti.
- FW_SERVICE_DNS (Firewall): se lavorate con un server dei nomi che deve essere accessibile dall'esterno, immettete qui yes; e contemporaneamente, per quel riguarda FW_TCP_SERVICES_* deve essere attivata la porta 53.
- FW_SERVICE_DHCLIENT (Firewall): se usate dhclient per ottenere il vostro indirizzo IP, immettete qui yes.
- FW_LOG_*: indicate qui cosa volete protocollare. Di solito basta yes in FW_LOG_DENY_CRIT .
- FW_STOP_KEEP_ROUTING_STATE (Firewall): se vi collegate automaticamente ad Internet tramite diald o ISDN (dial on demand), impostate qui yes.

A questo punto la configurazione è conclusa. Non dimenticate di testare il firewall (p.e. collegamento tramite telnet dall'esterno); in /var/log/messages dovrebbero apparire più o meno le seguenti comunicazioni:

```
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)
```

Configurazione con YaST

Tramite il centro di controllo diYaST potrete eseguire la configurazione assistita da YaST nella modalità grafica. Selezionate nella categoria 'Sistema ed utente' la voce 'Firewall'. La configurazione è suddivisa in quattro segmenti:

Impostazioni di base Determinate l'interfaccia da proteggere. Se si tratta di un singolo host senza una rete interna alle spalle, immette solo l' interfaccia esterna. Se vi è una rete indicate l'interfaccia interna . Uscite da questo dialogo cliccando su 'Prossimo'.

Servizi Questa opzione è rilevante solo se il vostro sistema debba offrire dei servizi accessibili via Internet, come ad esempio server web e di posta etc. Abilitate le relative caselle e/o attivate tramite 'Per esperti ...' determinati servizi indicando la relativa porta (che trovate in `/etc/services`). Se il vostro computer non deve fungere da server, lasciate questo dialogo senza apportare alcuna modifica cliccando su'Prossimo'.

Funzionalità Qui selezionate le principali funzionalità del vostro firewall:

- 'Permetti traceroute' per monitorare il routing verso il vostro firewall.
- 'Inoltra i dati ed effettua il mascheramento' protegge gli host sulla rete interna da attacchi provenienti da Internet — apparentemente è il vostro firewall ad utilizzare i servizi di Internet, mentre gli host della vostra rete interna rimangono invisibili.
- 'Proteggi tutti i servizi in esecuzione' significa che tutti gli accessi tramite rete ai servizi TCP e UDP del firewall saranno proibiti, ad eccezione di quelli che avete esplicitamente attivato nella finestra precedente.
- 'Proteggi dalla rete interna' Solo i servizi che non vengono bloccati dal firewall sono accessibili per gli host *interni*. Dato che qui non è possibile attivare dei servizi dovreste disattivare questa opzione se volete permettere l'accesso dalla rete interna.

Dopo aver configurato le funzionalità procedete con 'Prossimo'.

Opzioni di registrazioni Qui stabilite il volume delle comunicazioni di log del vostro firewall. Prima di attivare 'Opzioni di debug' considerate che questi file di log sono molto voluminosi. Dopo aver configurato anche questo aspetto, avete concluso la configurazione del vostro firewall. Lasciate il dialogo con 'Prossimo' e confermate l'avviso che verrà visualizzato per l'abilitazione del firewall.

19.2 SSH – secure shell, l'alternativa sicura

Lavorare in rete spesso comporta dover accedere ad host remoti. L'utente deve autenticarsi tramite il proprio nome di login e password. Se questi da-

ti non vengono cifrati possono venir intercettati da terzi e utilizzati per eseguire il login all'insaputa dell'utente. A parte il fatto che l'intrusore viola così la privacy dell'utente, 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; insicuri sono anche i semplici collegamenti FTP o collegamenti realizzati per copiare dei dati da un host all'altro.

Il software SSH offre la protezione necessaria. Il processo di autenticazione, di solito il nome utente e la password e il processo di comunicazione avvengono in forma cifrata; anche qui è possibile intercettare dei dati trasmessi ma senza la chiave il contenuto non può venire decifrato. Questo rende possibile una comunicazione sicura attraverso una rete insicura come Internet. SUSE LINUX offre il pacchetto OpenSSH.

19.2.1 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.

19.2.2 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. A causa della sua affinità con rlogin, il nome simbolico slogin punta anche su ssh. Per fare un esempio: con il comando `ssh sole`, si può accedere al computer 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 di utente locale e quello sul sistema remoto differiscono, potete indicare un nome differente p.es. `ssh -l agosto sole` oppure `ssh agosto@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 viene creata una directory con il nome `tmp`. L'output del programma avviene sul terminale locale del computer terra.

```
ssh sole "uptime; mkdir tmp"
tux@password_di_sole:
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 computer sole.

19.2.3 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 lamialettera.tex sole:` copia il file `lamialettera.tex` dal computer terra sul computer sole. Se i nomi di utente su terra e `sole` sono diversi, usate con scp la sintassi `nomeutente@nomecomputer`. Non esiste un'opzione `-l`.

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 incrementa da sinistra a destra. Inoltre, sul margine destro viene mostrato il tempo rimanente (stimato) per la trasmissione *estimated time of arrival*. Ogni output può venire soppresso con l'opzione `-q`.

scp offre, oltre alla copia di singoli file, anche un procedimento ricorsivo per la trasmissione di complete directory: `scp -r src/ sole:backup/` copia l'intero contenuto della directory `src/` sottodirectory inclusi su sole e lì nella sottodirectory `backup/` che viene generata automaticamente se ancora non dovesse esistere.

Per mezzo dell'opzione `-p`, scp conserva 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 carico di sistema più elevato.

19.2.4 sftp - trasmissione più sicura

Alternativamente, si può usare sftp per una trasmissione dei dati più sicura. Una sessione sftp offre molti dei comandi noti di ftp. Rispetto a scp si rivela vantaggioso soprattutto quando si trasmettono dati di cui non si conoscono i nomi di file.

19.2.5 Il demone SSH (sshd): lato sever

Affinché possano venire utilizzati ssh e scp, i programmi client del pacchetto SSH, deve girare in background il demone di SSH in ascolto sulla `porta 22 TCP/IP`.

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 il procedimento come procedimento basato su chiave pubblica. Per garantire una comunicazione sicura tramite SSH, solo l'amministratore deve poter prendere atto dei file delle chiavi private. A questo scopo, i permessi dei file vengono impostati (preimpostati) in modo molto restrittivo. Le chiavi private sono necessarie solo localmente al demone SSH e non possono venir trasmesse a nessun altro. Le chiavi pubbliche (riconoscibili dall'estensione `.pub`), invece, possono essere trasmesse al proprio interlocutore e sono di conseguenza 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 `host key` pubblica ed una `server key` che viene generata dal demone ad intervalli regolari di una ora. Per mezzo delle due chiavi, il client SSH crea una chiave di sessione, *session key* da lui liberamente scelta e la invia al server SSH: inoltre comunica al server il metodo di cifratura utilizzato *cipher* usato.

Il protocollo SSH versione 2 non prevede l'uso della `server key`. Al suo posto viene utilizzato l'algoritmo secondo Diffie-Hellman per lo scambio delle chiavi.

Le chiavi private host e server, 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 (cfr. `man /usr/share/doc/packages/openssh/RFC.nroff`). Questa fase iniziale di collegamento, può essere ricostruita facilmente tramite l'opzione `-v`, per la ricerca degli errori, del programma client di SSH. Di default viene utilizzato il protocollo SSH versione 2; con il parametro `-1` potete forzare l'uso del protocollo SSH versione 1. Se il client archivia tutte le host key pubbliche in `~/.ssh/known_hosts` in tal modo è possibile respingere attacchi del tipo man-in-the-middle. I server SSH che cercano di simulare il

nome ed indirizzo IP di un altro, vengono smascherati con un chiaro avviso a causa di una chiave host divergente da `~/.ssh/known_hosts` oppure per non sono in grado di decifrare la chiave convenuta della sessione, dal momento che non dispongono della 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'avvertimento poco rassicurante. Una volta accertato che, nonostante l'avviso, si tratta del server SSH giusto, eliminate la registrazione relativa a questo sistema da `~/.ssh/known_hosts`.

19.2.6 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 così 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 la chiave:

```
Enter file in which to save the key (/home/tux/.ssh/id_rsa):
```

Confermate il valore di default e stabilite una 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 memorizzate, ovvero, nel nostro esempio, nei file `id_rsa` e `id_rsa.pub`.

```
Enter same passphrase again:
Your identification has been saved in /home/bspuser/.ssh/id_rsa
Your public key has been saved in /home/bspuser/.ssh/id_rsa.pub.
The key fingerprint is:
79:c1:79:b2:e1:c8:20:c1:89:0f:99:94:a8:4e:da:e8 tux@sole
```

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 computer remoto, dove la salvate come `~/.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'X completo, viene avviato come processo figlio di ssh-agents. Potete realizzare ciò semplicemente impostando la variabile `usessh` - che si trova all'inizio del file `.xsession` - su `yes`, ed eseguire il login tramite un display manager (p.es.KDM o XDM). Alternativamente potete usare ssh-agentstartx.

Ora potete utilizzare ssh o scp. Se avete distribuito la vostra chiave pubblica, non dovreste più ricevere la richiesta d'inserimento della password. Quando uscite dal vostro computer, fate attenzione a terminare la vostra X session o bloccarla tramite un blocco dello schermo protetto da 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`.

19.2.7 Rideriggere X, l'autenticazione ed altro

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 computer di partenza. Questa comoda funzione previene contemporaneamente la possibilità d'intercettazione esistente finora nelle applicazioni-X lanciate su un computer remoto e visualizzate sul computer locale.

Tramite l'opzione `-A`, viene adottato il meccanismo di autenticazione ssh-agent dal prossimo computer. È così possibile passare da un computer all'altro senza dover inserire una password; questo però, solo se prima sono state distribuite e archiviate correttamente le chiavi pubbliche sui computer 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 qualsiasi collegamento TCP/IP. Come esempio riportiamo l'inoltro della porta SMTP e POP3:

```
ssh -L 25:sole:25 terra
```

Ad ogni collegamento indirizzato alla terra porta 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 mail possono in tal maniera venir inviate da una postazione qualsiasi con un collegamento di rete per essere consegnate dal server di posta proprio. In modo analogo con il seguente comando le richieste POP3 (porta 110) indirizzate al terra possono venir reindirizzate sulla porta POP3 di sole

```
ssh -L 110:sole:110 terra
```

Questi comandi vanno eseguiti come utente `root`, poiché vengono indirizzate porte locali privileggiate. Con un collegamento SSH esistente, la posta viene spedita e ritirata come 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`.

19.3 Autenticazione nella rete — Kerberos

Una rete aperta non offre oltre al comune meccanismo della password — già di per sé non sicurissimo — nessuna altra possibilità che permetta alla postazione di lavoro di identificare in modo sicuro l' utente. Ciò significa che non è da escludere che un utente appropriandosi dell'identità di un altro possa leggere le sue e-mail, accedere ai suoi file privati o inizializzare dei processi del sistema. La vostra rete deve soddisfare i seguenti criteri per dirsi veramente sicura:

- Gli utenti devono comprovare la propria identità prima di avviare dei servizi del sistema e assicuratevi che nessuno possa assumere l'identità di un altro.

- Inoltre, fate in modo che ogni server di rete dia prova della propria identità. Altrimenti un intruso potrebbe riuscire a fingere di essere il server a cui rivolgete le vostre richieste ed intercettare informazioni riservate che inviate al server. Per evitare questo vi è la cosiddetta "mutual authentication", ovvero autenticazione reciproca tra client e server.

Kerberos vi aiuta a realizzare quanto appena descritto grazie all'autenticazione cifrata. I seguenti paragrafi vi mostreranno la procedura da seguire. Comunque il modo di funzionare di Kerberos verrà descritto solo nei suoi principi. Per maggior dettagli anche di natura tecnica consultate la documentazione acclusa di Kerberos.

Nota

Il Kerberos originario è stato sviluppato al MIT (Massachusetts Institute of Technology). Oltre al MIT Kerberos vi sono anche altre implementazioni di Kerberos. SUSE LINUX contiene l' implementazione libera di Kerberos 5, il cosiddetto Heimdal Kerberos 5 di KTH. Visto che quanto descritto di seguito si riferisce alle caratteristiche comuni delle diverse implementazioni parleremo sempre di Kerberos, fatta eccezione per informazioni specifiche riguardanti Heimdal.

Nota

19.3.1 La terminologia di Kerberos

Prima di entrare nei particolari per quanto riguarda Kerberos, diamo uno sguardo al glossario riportato di seguito. Vi aiuterà ad orientarvi nella terminologia di Kerberos.

Credential Gli utenti o i client devono disporre dei credenziali che gli conferiscono il diritto di richiedere dei servizi. Kerberos ha due tipi di credenziali — i ticket e gli authenticator.

Ticket Il ticket documenta al server il diritto del client - che cerca di autenticarsi nei confronti dello stesso server - di richiedere dei servizi. Il ticket contiene il nome del server, il nome del client, l'indirizzo Internet del client, e un cosiddetto *timestamp*, ovvero la datazione del file, la validità e un chiave di sessione *session key* generata casualmente. Questi dati vengono cifrati con la chiave del server.

Authenticator Assieme al ticket viene utilizzato un authenticator per dimostrare che il client che presenta il ticket sia effettivamente quello che dichiara di essere. L'authenticator viene generato in base al nome del client, l'indirizzo IP della postazione di lavoro e l'orario attuale della postazione di lavoro— cifrato con la chiave di sessione nota solamente al client e al server a cui si rivolge il client per richiede un servizio. Contrariamente al ticket, l'authenticator può essere utilizzato una sola volta. Il client può generare da sé un authenticator.

Principal In Kerberos si tratta di una unità univoca (un utente o un servizio) a cui può essere assegnato un ticket. Un principal è composto da:

- **Primary** – La prima parte del principal che nel caso di un utente può essere identico al nome dell'utente.
- **Instance** – Informazione facoltativa che descrive la primary. Questa sequenza di caratteri è divisa dalla primary attraverso un `/`.
- **Realm** – Il realm stabilisce la vostra area Kerberos. Di solito il vostro realm è il vostro nome di dominio scritto in maiuscole.

Mutual Authentication Kerberos esegue un processo detto di autenticazione reciproca tra server e client che condividono una chiave di sessione grazie alla quale si ha la certezza dell'identità della controparte.

Session Key Le chiavi di sessione sono chiavi private temporanee generate da Kerberos. Sono note al client e vengono utilizzate per cifrare la comunicazione tra client e il server da cui il client ha richiesto e ottenuto un ticket.

Replay Quasi tutti i messaggi che vengono inviati in una rete possono essere intercettati, sottratti e inviati nuovamente. Per quanto riguarda Kerberos questo potrebbe rilevarsi pericoloso se l'intruso dovesse riuscire a intercettare le vostre richieste di servizi contenenti il vostro ticket ed authenticator. Potrebbe tentare di inviarle nuovamente ("replay") e spacciarsi per voi. Comunque Kerberos prevede diversi meccanismi per prevenire questa eventualità.

Server o service Un "service" viene utilizzato se deve essere eseguita una determinata azione, il processo sottostante si chiama "server".

19.3.2 Come funziona?

Kerberos viene spesso chiamato anche servizio di autenticazione "Trusted Third Party" che indica che i client, per quanto riguarda l'identità di un altro client, fanno affidamento sulla valutazione di Kerberos. Kerberos gestisce una banca dati con tutti gli utenti e le loro chiavi privati.

Per non avere delle brutte sorprese, il server di autenticazione e il server di ticket-granting devono girare su una macchina dedicata. Fate in modo che solo l'amministratore possa accedervi fisicamente e tramite la rete; limitate il più possibile il numero dei servizi di rete che girano su questo server — non fatevi girare neanche sshd.

Il primo contatto Entrare in contatto con Kerberos assomiglia al log-in su un comune sistema di rete. Immettete il vostro nome utente. Queste informazioni e il nome del Ticket- Granting Service abbreviato con TGS vengono inviate al server di autenticazione (Kerberos). Se il server di autenticazione sa della vostra esistenza, genera una chiave di sessione casuale per l'ulteriore scambio di dati il vostro client e il ticket granting server. A questo punto il server di autenticazione creerà a sua volta un ticket per il ticket granting server. Il ticket contiene le seguenti informazioni tutte cifrate con una chiave di sessione nota solo al server di autenticazione e a quello di ticket granting:

- Il nome del client e del ticket granting server
- L'ora attuale
- Il periodo di validità assegnata al ticket
- L'indirizzo IP del client
- La nuova chiave di sessione generata

Successivamente il ticket viene rimandato assieme alla chiave di sessione in forma cifrata al client, però utilizzando la chiave privata del client. Questa chiave privata è nota solo a Kerberos e al client, visto che è stata derivata dalla vostra password. Non appena il client ottiene questa risposta, vi verrà chiesta la password. La password verrà convertita nella chiave capace di decifrare il pacchetto inviato dal server di autenticazione. Il pacchetto viene scompattato, e sia la password che la chiave vengono cancellati dalla memoria della postazione di lavoro. La vostra workstation può comprovare la vostra identità per la durata della validità del ticket granting ticket abbreviato con TGT.

Richiesta di un servizio Per poter richiedere un servizio da un server qualsiasi sulla rete, l'applicazione del client deve dimostrare la propria identità. Così l'applicazione genera un authenticator che è composto da:

- il principal del client
- l'indirizzo IP del client
- l'ora attuale
- la somma di controllo (determinata dal client)

Tutte queste informazioni vengono cifrate con la chiave di sessione che il client ha già ricevuto per questo server in particolare. L'authenticator e il ticket per il server vengono inviati al server. Il server utilizza la propria copia della chiave di sessione per decifrare l'authenticator che gli fornisce una serie di informazioni necessarie sul client richiedente un servizio. Queste informazioni vengono comparate a quelle contenute nel ticket. In tal modo il server verifica se il ticket e l'authenticator provvengono dallo stesso client.

Se sul lato server non vi fossero delle misure di sicurezza, questo passaggio sarebbe quello ideale per sferrare un attacco replay. Qualche "pirata della rete" potrebbe tentare di inviare nuovamente una richiesta che è stata intercettata precedentemente sulla rete. Per evitare ciò, il server non accetta richieste con una datazione e ticket già ricevuti. Inoltre possono essere rifiutate le richieste la cui datazione si discosta notevolmente dal momento della ricezione.

Autenticazione reciproca L'autenticazione di Kerberos può essere impiegata in entrambi le direzioni. Non si tratta solo di stabilire se il client è veramente quello che dichiara di essere; anche il server deve essere in grado di autenticarsi di fronte al client che richiede un determinato servizio. Così anche il server invia una specie di authenticator. Aggiunge 1 alla somma di prova ottenuta dall'authenticator del client ed esegue la cifratura con la chiave della sessione condivisa con il client. Il client considera questa risposta come prova della veracità dell'identità del server, e può avere inizio lo scambio di dati tra client e server.

Ticket-Granting — presa di contatto con tutti i server
I ticket valgono per un server; questo significa che appena richiedete un altro servizio avrete bisogno di un altro ticket. Kerberos implementa un meccanismo per la generazione di ticket per i singoli server. Questo servizio viene chiamato "Ticket-Granting Service"

che si potrebbe tradurre con: servizio di emissione di ticket. Questo servizio è un servizio come tutti gli altri e sottosta di conseguenza agli stessi protocolli di accesso sovramenzionati. Ogni volta che ad una applicazione serve un ticket, per cui non vi sono altre richieste, essa entra in contatto con il server per l'emissione dei ticket. La richiesta è composta da:

- Il principal richiesto
- Il ticket granting ticket (TGT)
- L'authenticator

Come nel caso di ogni altro server, il ticket granting server verifica il TGT e l'authenticator. Se vengono riconosciuti come validi, il server di ticket granting genera una nuova chiave di sessione per il client originario e il nuovo server. Successivamente viene generato il ticket per il nuovo server contenente le seguenti informazioni:

- Il principal del client
- Il principal del server
- L'ora attuale
- L'indirizzo IP del client
- La nuova chiave di sessione appena generata

Al nuovo ticket viene assegnato un periodo di validità che corrisponde al rimanente periodo di validità del TGT o al valore standard per il servizio, a seconda di cosa sia più breve. Questo ticket e la chiave di sessione vengono inviati al client dal servizio di emissione di ticket (TGS). Questa volta però la risposta è stata cifrata dalla chiave di sessione che è stata ricevuta assieme al TGT originario. Quando viene richiesto un altro servizio, il client è in grado di decifrare la risposta senza richiedere nuovamente la password dell'utente. In questo modo Kerberos ottiene per il client un ticket dopo l'altro senza che l'utente debba eseguire ogni volta il login.

Compatibilità con Windows 2000 Windows 2000 contiene una implementazione Microsoft di Kerberos 5. Visto che SUSE LINUX usa l'implementazione Heimdal di Kerberos 5, nella documentazione di Heimdal troverete sicuramente delle utili informazioni ed ulteriori istruzioni; vedi la sezione 19.3.4 a pagina 499.

19.3.3 Kerberos e l'utente

Nel caso ideale l'utente viene confrontato con Kerberos solo al momento del login sulla sua postazione di lavoro. Al login ottiene un TGT; al logout i ticket Kerberos dell'utente vengono distrutti automaticamente per evitare che altri utenti possano spacciarsi per questo utente quando questi è uscito dal sistema. Il fatto che i ticket vengono distrutti automaticamente comporta delle difficoltà se la sessione dell'utente supera nella durata il periodo di validità assegnato al TGT (10 ore sono un buon valore indicativo). L'utente può ottenere un nuovo TGT, inizializzando kinit. Basta immettere nuovamente la password — e Kerberos farà in modo che l'utente potrà accedere ad ogni servizio che richiede senza dover autenticarsi di nuovo. Coloro che sono interessati ad avere un elenco di tutti i ticket che Kerberos ha ottenuto per voi in background, ricoreranno a klist.

Segue una selezione di applicazioni che utilizzano l'autenticazione Kerberos. Queste applicazioni si trovano sotto `/usr/lib/heimdal/bin`. Tutte queste applicazioni offrono tutte le funzionalità delle applicazioni note di UNIX/Linux ed inoltre il vantaggio di una autenticazione trasparente grazie a Kerberos:

- telnet/telnetd
- rlogin
- rsh, rcp, rshd
- popper/push
- ftp/ftpd
- su
- imapd
- pine

Come noterete non dovrete immettere la vostra password per poter utilizzare queste applicazioni, poiché Kerberos ha già dimostrato la vostra identità. ssh — se compilato per supportare Kerberos — riesce addirittura ad inoltrare ad un'altra postazione di lavoro tutti i ticket che avete ottenuto per una determinata postazione di lavoro. Se utilizzate ssh per fare il login su di un'altra postazione di lavoro, ssh adatterà i contenuti cifrati dei ticket alla nuova situazione. Non basta copiare i ticket semplicemente da una postazione all'altra, visto che il ticket contiene informazioni specifiche

della postazione (l'indirizzo IP). XDM e KDM supportano anche Kerberos. Leggete nella *Kerberos V5 UNIX User's Guide* all' `http://web.mit.edu/kerberos/www/krb5-1.3/krb5-1.3/doc/krb5-user.html` di più sulle applicazioni di rete di Kerberos.

19.3.4 Ulteriori informazioni su Kerberos

SUSE LINUX contiene la libera implementazione di Kerberos, chiamata Heimdal. La documentazione relativa viene installata con il pacchetto `heimdal` sotto `/usr/share/doc/packages/heimdal/doc/heimdal.info`. La documentazione si trova anche su Internet: `http://www.pdc.kth.se/heimdal/`.

Sulla pagina web ufficiale della implementazione Kerberos del MIT trovate dei link ad altre risorse relative a Kerberos:`http://web.mit.edu/kerberos/www/`

Una spiegazione del modo di funzionare di Kerberos, e non solo vertente sugli aspetti tecnici, molto interessante è il dialogo che trovate sotto: `http://web.mit.edu/kerberos/www/dialogue.html`

Questo documento spiega il modo fondamentale di funzionamento di Kerberos in modo ben comprensibile. Inoltre contiene una serie di indicazioni per trovare ulteriori fonti di informazione su Kerberos:`ftp://athena-dist.mit.edu/kerberos/doc/usenix.PS`

Nelle URL riportate di seguito viene introdotto Kerberos, risposto a tante domande concernenti l'installazione, la configurazione e l'amministrazione di Kerberos: `http://web.mit.edu/kerberos/www/krb5-1.3/krb5-1.3/doc/krb5-user.html`

`http://web.mit.edu/kerberos/www/krb5-1.3/krb5-1.3/doc/krb5-install.html`

`http://web.mit.edu/kerberos/www/krb5-1.3/krb5-1.3/doc/krb5-admin.html`

L'FAQ su Kerberos ufficiale: `http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html`

Tung, Brian: *Kerberos — A Network Authentication System*. Addison Wesley, 1999. - (ISBN 0-201-37924-4)

19.4 Installare e amministrare Kerberos

Questa sezione tratta l'installazione della implementazione Kerberos Heimdal e alcuni aspetti riguardanti l'amministrazione. Si parte dal presuppo-

sto che disponete già delle nozioni basilari in tema Kerberos (vedi anche la sezione 19.3 a pagina 492).

19.4.1 Stabilire i realm di Kerberos

Il domain di una installazione Kerberos viene chiamato realm e viene identificato con un nome tipo `FOOBAR.COM` o semplicemente `ACCOUNTING`. Kerberos distingue tra maiuscole e minuscole, dunque `foobar.com` è un realm diverso da `FOOBAR.COM`. Usate le maiuscole o minuscole secondo le vostre preferenze. Comunque di solito vengono usate le maiuscole per nomi di realm.

Potete usare anche il vostro nome di dominio DNS (oppure un sottodominio, p.e. `ACCOUNTING.FOOBAR.COM`). Come vedremo di seguito, se siete un amministratore di sistema potete semplificarvi la vita configurando i client Kerberos in modo che accedono al KDC ed ad altri servizi diKerberos via DNS. Per realizzare ciò, è bene che il nome del realm sia un sottodominio del vostro nome di dominio DNS.

Diversamente dall'area dei nomi DNS, Kerberos è non strutturato in modo gerarchico. Non potete settare un realm nominato `FOOBAR.COM`, avere due sottorealm nominati `DEVELOPMENT` e `ACCOUNTING` e aspettarvi che i due realm subordinati ereditano in qualche modo i principal di `FOOBAR.COM`. Avrete invece tre realm a sé stanti per i quali dovreste configurare l'autenticazione crossrealm in modo che gli utenti di un realm possano interagire con un server o con utenti di un altro realm. Come settare l'autenticazione crossrealm è descritto p.e. in [15] (Tung).

Per motivi di semplicità partiamo dal presupposto che settate solo un realm per l'intera azienda od istituzione simile. In questa sezione useremo in tutti gli esempi il nome di realm `SAMPLE.COM`.

19.4.2 Impostare l'hardware KDC

Per poter usare Kerberos la prima cosa che vi serve è una macchina che funge da Key Distribution Center abbreviato con KDC, contente l'intera banca dati degli utenti di Kerberos assieme alle password e alle altre informazioni.

Il KDC è la componente più importante dell'intera infrastruttura di sicurezza — se qualcuno riesce ad entrarvi in modo non autorizzato, tutti gli account degli utenti e l'intera infrastruttura protetta da Kerberos è compromessa. Un hacker con accesso alla banca dati di Kerberos può assumere le

sembianze di un principal qualsiasi nella banca dati! Fate in modo che le misure di sicurezza per questo computer siano quanto serveri possibili:

- Mettete il server in un luogo sicuro, per esempio in una stanza per server tenuta sotto chiave a cui hanno accesso solo un numero ristretto di persone.
- Dedicate il server esclusivamente al KDC. Questo vale per applicazioni sia server che client — il KDC per esempio non dovrebbe importare alcun file system tramite NFS o non dovrebbe usare DHCP per ottenere la propria configurazione di rete.

  Si consiglia di installare prima il sistema minimale, controllare poi la lista dei pacchetti installati e rimuovere quindi i pacchetti non necessari, particolare server come inetd, portmap e cups e tutto quanto ha a che fare con X11. Anche installare un server ssh comporta un rischio in termini di sicurezza. Non è possibile eseguire un login grafico su questa macchina perché un X server rappresenta un potenziale rischio di sicurezza. Kerberos ha comunque una propria interfaccia di amministrazione.
- Configurate `/etc/nsswitch.conf` in modo che la ricerca di utenti e gruppi venga effettuata solo nei file locali. Modificate le righe per `passwd` e `group` nel seguente modo:

  ```
  passwd:         files
  group:          files
  ```

  Editate i file `passwd`, `group`, `shadow` e `gshadow` in `/etc` e cancellate le righe che iniziano con un `+` (per richieste NIS).

  Considerate anche la possibilità di disabilitare le richieste DNS per motivi di sicurezza. Se la libreria resolver di DNS presenta una falla nella sicurezza, un aggressore potrebbe riuscire a far eseguire al KDC una richiesta DNS che sfrutti questa falla. Per disabilitare richieste DNS, cancellate semplicemente `/etc/resolv.conf`.
- Disabilitate tutti gli account degli utenti fatta eccezione per l'account di root editando `/etc/shadow` e sostituendo al valore hash delle password `*` o `!`.

19.4.3 Sincronizzazione dell'orario

Per usare Kerberos in modo efficace provvedete a sincronizzare l'orario dei sistemi. La ragione è che Kerberos cerca di proteggervi da cosiddetti credenziali (replayed) cioè inviati più volte. Un intruso potrebbe intercettare i credenziali di Kerberos nella rete e riutilizzarli per sferrare degli attacchi contro il server. Kerberos implementa diversi meccanismi per prevenire questa eventualità, uno dei quali consiste nell' aggiungere dei time stamp ovvero la datazione ai ticket. Un server che riceve un ticket con una datazione non attuale rifiuterà il ticket.

Chiaramente Kerberos consente una certa discrepanza tra le datazioni. Comunque gli orologi dei computer possono essere poco precisi nello scandire il tempo — non accade di rado che orologi di PC guadagno o perdono mezz'ora nell'arco di una settimana rispetto all'orario di riferimento. Si consiglia dunque di configurare tutti gli host nella rete in modo che si sincronizzano sull'orario impostato centralmente.

Un modo semplice per farlo è quello di installare un server dell'orario NTP su una macchina e sincronizzare l'orario dei vari client su quello di questo server, facendo girare un demone NTP nel modo client su tutte le macchine o eseguendo `ntpdate` una volta al giorno su tutti i client (questa soluzione probabilmente è praticabile solo con un numero limitato di client).

Anche il KDC deve essere sincronizzato sull'ora centrale. Far girare un demone NTP su questa macchina rappresenterebbe un rischio in termini di sicurezza, per questo si consiglia di sincronizzare l'ora lanciando `ntpdate` tramite una registrazione cron.

La configurazione dell'NTP non rientra nel quadro di questa sezione, per avere ulteriori informazioni consultate la documentazione su NTP che trovate acclusa sotto `/usr/share/doc/packages/xntp-doc`.

Chiaramente potete impostare il livello di tolleranza di Kerberos per quando riguarda lo scarto tra le datazioni (*time stamps*) secondo le vostre preferenze. La variabile (`clock skew`) si imposta nel file di configurazione `krb5.conf`, come descritto nella sezione 19.4.6 a pagina 508.

19.4.4 Configurazione dell'attività di log

Di default, i demoni Kerberos che girano sull' host KDC protocollano le informazione riguardanti il demone syslog. Se volete tenere sott'occhio l'attività di KDC, controllate questi file di protocollo ad intervalli regolari per vedere se si verificano delle stranezze o se potrebbero insorgere dei possibili problemi.

Per farlo eseguite uno script di scansione dei log sull'host KDC o copiate questi file di log dal KDC su un altro host, ed analizzate lì i file di log. Si sconsiglia di inoltrare l'output di log tramite il meccanismo di inoltro di syslogd, perché le informazioni attraversano la rete in forma non cifrata.

19.4.5 Installare il KDC

In questa sezione verrà descritta l'installazione di KDC e la configurazione di un principal amministrativo.

Installare gli RPM

Innanzitutto bisogna installare il software Kerberos. Installate gli rpm `heimdal`, `heimdal-lib` e `heimdal-tools` sul KDC:

```
$> rpm -ivh heimdal-*.rpm heimdal-lib-*.rpm heimdal-tools*.rpm
```

Impostare la cosiddetta chiave master

Ora dovete inizializzare la banca dati nella quale Kerberos raccoglie tutte le informazioni sui principal. Innanzitutto impostate la chiave master utilizzata per proteggervi contro la fuga accidentale di informazioni dalla banca di dati, in particolar modo quando eseguite un back-up su nastro.

La chiave master viene derivata da una pass phrase memorizzata in un file chiamato file stash. Quindi non è necessario immettere la password ad ogni riavvio di KDC. Scegliete la pass phrase con accortezza, p.e. la frase di un libro che si trova su una pagina aperta a caso.

Quando eseguite delle copie di sicurezza su nastro della banca dati di Kerberos(`/var/heimdal/heimdal.db`), non fatene una dello stash file (che è in `/var/heimdal/m-key`). Altrimenti chiunque è in grado di leggere il nastro potrebbe anche decifrare la banca dati. Per questo motivo è consigliabile tenere una copia della pass phrase in un luogo sicuro, visto che vi servirà quando dovrete ripristinare dal nastro la banca dati in seguito ad un crollo.

Per impostare la chiave master, invocate l'utility kstash senza ulteriori argomenti ed immettete la pass phrase due volte:

```
$> kstash
Master key:<enter pass phrase>
Verifying password - Master key:<enter pass phrase again>
```

Generare il realm

Infine immettete le vostre registrazioni per il realm nella banca dati di Kerberos. Inizializzate l'utility kadmin con l'opzione `-l`. Questa opzione dà l'istruzione a kadmin di accedere alla banca dati locale. Di default kadmin cercherà di contattare il servizio di amministrazione di Kerberos tramite la rete, il che al momento non funzionerebbe, visto che il servizio non è stato ancora inizializzato.

Ora date a kadmin l'istruzione di inizializzare il vostro realm. Vi verranno poste una serie di domande. All'inizio si consiglia di accettare quanto impostato di default da kadmin:

```
$> kadmin -l
kadmin> init SAMPLE.COM
Realm max ticket life [unlimited]: <press return>
Realm max renewable ticket life [unlimited]: <press return>
```

Per verificare cosa è accaduto, usate il comando list:

```
kadmin> list *
default@SAMPLE.COM
kadmin/admin@SAMPLE.COM
kadmin/hprop@SAMPLE.COM
kadmin/changepw@SAMPLE.COM
krbtgt/SAMPLE.COM@SAMPLE.COM
changepw/kerberos@SAMPLE.COM
```

Questo indica che nella banca dati vi sono una serie di principal destinati da Kerberos per l'uso interno.

Generare un principal

Ora generate due principal Kerberos per voi stessi: un principal normale per le mansioni quotidiane e uno per compiti amministrativi riguardanti Kerberos. Assumendo che il vostro nome di login sia `newbie`, procedete come riportato di seguito:

```
$> kadmin -l
kadmin> add newbie
Max ticket life [1 day]: <press return>
Max renewable life [1 week]: <press return>
Principal expiration time [never]: <press return>
Password expiration time [never]: <press return>
Attributes []: <press return>
newbie@SAMPLE.COM's Password: <type password here>
Verifying password: <re-type password here>
```

Potete accettare i valori di default premendo Enter. Scegliete una password adatta.

Dopo generate un altro principal chiamato `newbie/admin` inserendo `addnewbie/admin` al prompt di `kadmin`. Il suffisso `admin` in questo caso indica il ruolo *role* che vi permetterà di amministrare la banca dati di Kerberos.

Un utente può assumere diversi ruoli per scopi diversi, che comunque non ha niente a che vedere con la magia — considerateli piuttosto degli account del tutto diversi con un nome simile.

Avviare il KDC

Avviate i demoni KDC, ciò include kdc (il demone che gestisce l'autenticazione degli utenti e le richieste di ticket), kadmind (il server per l'amministrazione remota) e kpasswd (che gestisce le richieste degli utenti per la modifica della password). Per avviare il demone manualmente, immettete:

```
$> rckdc start
Starting kdc                done
```

Assicuratevi che il KDC venga avviato di default quando viene riavviato il server. Il comando è `insserv kdc`.

19.4.6 Configurare client Kerberos

Ci sono due modi per configurare Kerberos — configurazione statica tramite il file `/etc/krb5.conf` o configurazione dinamica tramite DNS. Nella variante DNS, le applicazioni di Kerberos cercheranno di accedere ai servizi di KDC tramite registrazioni DNS. Mentre nell' approccio statico dovete immettere i nomi degli host del vostro server KDC nel file `krb5.conf` (e aggiornare il file ogni volta che spostate il KDC o riconfigurate il vostro realm).

La configurazione tramite DNS è in genere molto più flessibile e meno laboriosa. Comunque il nome di realm deve essere lo stesso del vostro dominio DNS o di un sottodominio di esso.

Configurare Kerberos tramite DNS inoltre crea un piccolo rischio di sicurezza: un intruso potrebbe danneggiare seriamente la vostra infrastruttura attraverso il vostro DNS (shoot down del server dei nomi, spoofing ovvero falsificazione delle registrazioni DNS etc). Nella peggior delle ipotesi avremo un denial of service. Qualcosa di simile può verificarsi anche nel caso della configurazione statica, a meno che in `krb5.conf` non immettiate indirizzi IP al posto dei nomi degli host.

La configurazione statica

Come già accennato, un modo per configurare Kerberos consiste nell'editare il file di configurazione `/etc/krb5.conf`. Il file è incluso di default nel sistema installato e contiene alcune registrazioni esempio. Cancellatele prima di iniziare con la vostra configurazione.

`krb5.conf` è composto da diverse sezioni. Ognuna di queste sezioni inizia con il nome della sezione riportata nelle parentesi quadre (`[nomeesempio]`).

Nel caso della configurazione statica, aggiungete le seguenti righe in `krb5.conf` (`kdc.sample.com` è il nome dell' host di KDC):

```
[libdefaults]
        default_realm = SAMPLE.COM


[realms]
        SAMPLE.COM = {
                kdc = kdc.sample.com
                kpasswd_server = kdc.sample.com
                admin_server = kdc.sample.com
        }
```

Tramite `default_realm` stabilite il realm di default per applicazioni Kerberos.

Se avete diversi realm, aggiungete semplicemente un ulteriore istruzione alla sezione `[realms]`.

Aggiungete anche una istruzione che indichi alle applicazioni come mappare i nomi degli host ai realm. Per esempio quando vi connettete ad un host remoto, la libreria Kerberos deve sapere in quale realm si trovi l'host. Ciò va impostato nella sezione `[domain_realms]`:

```
[domain_realm]
        .sample.com = SAMPLE.COM
        www.foobar.com = SAMPLE.COM
```

Questo indica alla libreria che tutti gli host nei domini DNS `sample.com` si trovano nel realm di Kerberos `SAMPLE.COM`. Inoltre un host esterno di nome `www.foobar.com` dovrebbe anch'esso essere considerato appartenente al realm `SAMPLE.COM`.

La configurazione basata su DNS

Nella configurazione basata su DNS di Kerberos vengono usate tante registrazioni SRV (vedi *(RFC2052) A DNS RR for specifying the location of services* all'indirizzo (`http://www.ietf.org`). Queste registrazioni non vengono supportate da implementazioni precedenti del server dei nomi BIND. Lo sono a partire dalla versione 8 di BIND.

Il nome di una registrazione SRV, per quanto riguarda Kerberos, è composta nel seguente modo: `_service._proto.realm`, laddove realm è il realm di Kerberos. Tenete presente che DNS non distingue tra maiuscole e minuscole nei nomi di dominio, mentre lo fanno i realm di Kerberos, che quindi non funzionerebbero con questo metodo di configurazione. `_service` è il nome del servizio (vengono usati differenti nomi quando si cerca per esempio di contattare il KDC o il servizio password). `_proto` può assumere il valore `_udp` o `_tcp`, ma non tutti i servizi supportano entrambi i protocolli.

La parte dei dati delle registrazioni di risorse SRV consiste di un valore di priorità, ponderazione, un numero di porta e di un nome di host. La priorità definisce l'ordine nel quale gli host devono essere contatti (valori bassi indicano un'alta priorità). La ponderazione serve ad avere un load balancing, ovvero un bilanciamento del carico di lavoro tra server di egual priorità. Probabilmente questa funzione non vi servirà, così potete impostarlo su zero.Heimdal Kerberos cerca i seguenti nomi quando cerca di rilevare dei servizi:

_kerberos che definisce la locazione del demone KDC (il server di autenticazione e di ticket granting). Delle registrazioni tipiche hanno il seguente aspetto:

```
_kerberos._udp.SAMPLE.COM.  IN  SRV    0 0 88 kdc.sample.com.
_kerberos._tcp.SAMPLE.COM.  IN  SRV    0 0 88 kdc.sample.com.
```

_kpasswd che indica la locazione del server per modificare la password. Registrazioni tipiche sono:

```
_kpasswd._udp.SAMPLE.COM.   IN  SRV    0 0 464 kdc.sample.com.
```

Visto che kpasswdd non supporta TCP, non ci dovrebbe essere alcuna registrazione `_tcp`.

_kerberos-adm che indica la locazione del server di amministrazione remoto. Ecco delle registrazioni tipiche:

```
_kerberos-adm._tcp.SAMPLE.COM. IN SRV 0 0 749 kdc.sample.com.
```

Visto che kadmind non supporta UDP, non ci dovrebbero essere registrazioni _udp.

Come per il caso del file di configurazione statico, vi è un meccanismo che informa i client che un host specifico si trova nel realm SAMPLE.COM, anche se non fa parte del dominio DNS sample.com. Questo può essere realizzato aggiungendo una istruzione TXT a _kerberos.nomehost, come mostrato di seguito:

```
_kerberos.www.foobar.com.  IN TXT "SAMPLE.COM"
```

Sincronizzare l'ora

Con la variabile clock skew impostate i limiti entro i quali si accettono ticket la cui datazione si discosta dall'ora del sistema host.

Di solito si indicano 300 secondi (5 minuti). Dunque ticket con una discrepanza di cinque minuti in avanti o in dietro rispetto all'ora del server vengono ancora accettati.

Se utilizzate NTP per sincronizzare l'orario degli host, questo valore può essere ridotto ad un minuto.

Editate la variabile clock skew in /etc/krb5.conf nel modo seguente:

```
[libdefaults]
          clockskew = 120
```

19.4.7 Impostare l'amministrazione da remoto

Per aggiungere o rimuovere dei principal dalla banca dati di Kerberos senza disporre dell'accesso diretto alla console del KDC, comunicate al server di amministrazione di Kerberos quali principal sono provvisti del permesso di farlo.

A tal fine editate il file /var/heimdal/kadmind.acl (ACL sta per Access Control List). Il file ACL consente di specificare i permessi e di ceselare il grado di controllo. Per ulteriori informazioni consultate la pagina di manuale (man 8 kadmind).

Conferitevi il permesso di fare tutto ciò che intendete realizzare nella banca dati aggiungendo il seguente rigo:

```
newbie/admin all
```

Sostituite newbie con il vostro nome utente. Riavviate il KDC per rendere effettive le modifiche.

Amministrazione da remoto tramite kadmin

Il tool kadmin vi permette di amministrare Kerberos da remoto. Innanzitutto si rende necessario un ticket per il vostro principal di amministrazione da usare quando vi collegate al server kadmin:

```
$> kinit newbie/admin
newbie/admin@SAMPLE.COM's Password: <enter password>

$> /usr/sbin/kadmin
kadmin> privs
change-password, list, delete, modify, add, get
```

Con il comando privs potete verificare i permessi di cui disponete. La lista indicata sopra riporta tutti i permessi di cui disponete.

Modificate per esempio il principal newbie:

```
kadmin> mod newbie
Max ticket life [1 day]:2 days
Max renewable life [1 week]:
Principal expiration time [never]:2003-01-01
Password expiration time [never]:
Attributes []:
```

Così avete modificato la validità massima del ticket portandola a due giorni, e avete impostato la data di scadenza dell'account per il primo gennaio del 2003.

I comandi principali di kadmin

Segue un breve elenco dei comandi principali di kadmin, per ulteriori dettagli consultate la pagina di manuale `kadmin(8)`.

add`principal` aggiunge un nuovo principal.

modify `principal` edita diversi attributi di un principal, come la validità massima del ticket e la scadenza dell'account.

delete `principal` rimuove un principal dalla banca dati.

rename `principal nuovo nome` cambia il nome del principal in nuovo nome.

list `pattern` elenca tutti i principal che presentano determinate caratteristiche. I pattern funzionano alla stregua dei globbing pattern della shell: `list newbie*` elencherebbe `newbie` e `newbie/admin` nel nostro esempio.

get `principal` mostra informazioni dettagliate sul principal.

passwd `principal` cambia la password del principal.

Ottenete dell'assistenza premendo in ogni momento su ? e Enter, anche al prompt dei comandi del tipo `modify` e `add`.

Il comando `init` che viene utilizzato quando il realm è stato generato la prima volta, e non è disponibile nella modalità remota. Per generare un nuovo realm, andate sulla console di KDC e usate kadmin nella modalità locale (con l'opzione di riga di comando `-l`).

19.4.8 Generare principal di hostKerberos

Ogni host all'interno di una rete deve essere incluso in un realm di Kerberos e poter contattare un KDC. Inoltre dovete creare anche un cosiddetto "host principal".

Finora abbiamo trattato solo i credenziali degli utenti. Servizi sì detti "kerberizzati" devono autenticarsi di solito anche di fronte all'utente del client. A tal fine vi sono dei cosiddetti "host principal" per tutti gli host all'interno di un realm nella banca dati di Kerberos.

La relativa convenzione di nome è: `host/<hostname>@<REALM>`, `hostname` è il nome completo valido dell'host interessato.

Gli host principal sono simili ai principal di utenti normali, la differenza principale tra principal dell'utente e principal dell'host è comunque che la chiave del principal dell'utente è protetta da una password. Quando un utente ottiene un TGT dal KDC, deve immettere la password affinché Kerberos possa decifrare il ticket. Per un amministratore di sistema sarebbe molto scomodo dover richiedere ogni otto ore nuovi ticket per il demone SSH.

Nel caso dei principal per gli host questo problema viene risolto nel modo seguente: la chiave necessaria al principal dell'host per decifrare il ticket originale viene richiesta una volta da parte dell'amministratore del KDC. Successivamente la chiave viene salvata in un file locale di nome `keytab`. Servizi come il demone SSH leggono questa chiave e la utilizzano per ottenere all'occorrenza automaticamente una nuova chiave. Il file standard `keytab` si trova sotto `/etc/krb5.keytab`.

Per creare un principal dell'host per `machine.sample.com`, immettete durante una sessione di kadmin quanto segue:

```
$> kinit newbie/admin
newbie/admin@SAMPLE.COM's Password: <type password>

$> kadmin add -r host/machine.sample.com
Max ticket life [1 day]:
Max renewable life [1 week]:
Principal expiration time [never]:
Password expiration time [never]:
Attributes []:
```

Invece di settare una password per il nuovo principal, l'opzione `-r` istruisce kadmin a generare una chiave casuale; in questo caso ciò è possibile visto che per questo principal non si prevede il login da parte degli utenti: si tratta di un puro account per server di questa macchina.

Infine viene estratta la chiave e la si salva nel file keytab locale `/etc/krb5.keytab`. Questo file appartiene al superutente dunque dovete diventare root per eseguire il seguente comando:

```
$> ktutil get host/machine.sample.com
```

In seguito distruggete il ticket di amministrazione ottenuto tramite kinit con il comando `kdestroy` come descritto sopra.

19.4.9 Abilitare il supporto PAM per Kerberos

SUSE LINUX contiene il modulo PAM `pam_krb5` che supporta il login via Kerberos e l' aggiornamento della password. Questo modulo può essere utilizzato da applicazioni come la console di login, 'su' e applicazioni grafiche come KDM, dove l'utente immette una password ed intende utilizzare il meccanismo di autenticazione per ottenere un ticket Kerberos.

A partire di questa versione di SUSE LINUX il modulo `pam_unix` supporta l'autenticazione Kerberos e modifiche di password. Per abilitare il supporto di kerberos `pam_unix` dovete modificare il file `/etc/security/pam_unix2.conf` come mostrato di seguito:

```
auth:       use_krb5 nullok
account:    use_krb5
password:   use_krb5 nullok
session:    none
```

Quando questo file viene analizzato, tutti i servizi utilizzano Kerberos per l'autenticazione degli utenti. Se un utente non dispone di un principal Kerberos, `pam_unix` ricorrerà al normale meccanismo di autenticazione basato sulla password. La password per Kerberos dovrebbe essere adesso aggiornabile in modo transparente con il comando `passwd`.

Per delle impostazioni mirate di `pam_krb5` editate il file `/etc/krb5.conf` e aggiungete applicazioni standard per `pam`. Il modo di procedere viene descritto dettagliatamente nella pagina di manuale (`man 5 pam_krb5`).

Il modulo `pam_krb5` **non** è stato concepito per servizi di rete che accettano ticket di Kerberos nel quadro del processo di autenticazione dell'utente — questa è tutta una tematica a cui dedicheremo i seguenti paragrafi.

19.4.10 Configurare SSH per l'autenticazione Kerberos

OpenSSH supporta l'autenticazione Kerberos sia nella versione di protocollo 1 che 2. La versione 1 utilizza un determinato tipo di messaggi di log per la trasmissione di ticket Kerberos. La versione 2 utilizza Kerberos non più in modo diretto ma ricorre al GSSAPI, *General Security Services API*. Questa interfaccia di programmazione non è limitata all'utilizzo con Kerberos. E' stata sviluppata per celare di fronte alla applicazione le caratteristiche del sistema di autenticazione che sta alla base, sia esso Kerberos, SPKM o un altro sistema paragonabile. Però, l'attuale libreria GSSAPI di SUSE LINUX supporta solo Kerberos.

Per usare sshd con l'autenticazione Kerberos, editate `/etc/ssh/sshd_config` ed impostate le seguenti opzioni:

```
      # These are for protocol version 1
KerberosAuthentication yes
KerberosTgtPassing yes
# These are for version 2
GSSAPIAuthentication yes
GSSAPIKeyExchange yes
```

In seguito, riavviate il demone SSH con `rcsshd restart`.

Se volete utilizzare l'autenticazione Kerberos con la versione di protocollo 2 dovete attivarne il supporto sul lato client, editando il file di configurazione `/etc/ssh/ssh_config` lo attivate per l'intero sistema, editando il file `~/.ssh/config` lo attivate a livello di utente. In entrambi i casi si aggiunge l'opzione `GSSAPIAuthentication yes` al file di configurazione.

A questo punto dovreste essere in grado di creare una connessione con l'autenticazione Kerberos. Con `klist` potete controllare se avete un ticket valido per la connessione con il server SSH. Per forzare l'uso del protocollo SSH versione 1 utilizzate l'opzione `-1` sulla riga di comando.

```
$> ssh earth.sample.com
Last login: Fri Aug  9 14:12:50 2002 from zamboni.sample.com
Have a lot of fun...
```

19.4.11 Utilizzare LDAP e Kerberos

Con Kerberos, LDAP rappresenta un modo di distribuire le informazioni riguardanti gli utenti (user ID, gruppi, directory home, etc.) nella rete locale. Chiaramente questo presuppone l'utilizzo di un meccanismo di cifratura sicuro per evitare lo spoofing di pacchetti. Potrete utilizzare Kerberos per lo scambio di dati LDAP.

OpenLDAP implementa la maggior parte dei diversi modi di autenticazione tramite SASL, *Simple Authentication Session Layer*. SASL è in fondo un protocollo di rete per l'autenticazione. SUSE LINUX utilizza l'implementazione cyrus-sasl e supporta diversi modi di autenticazione. L'autenticazione Kerberos viene realizzata tramite GSSAPI (General Security Services API).

Di default il plug-in SASL per GSSAPI non è installato, dovete installarlo manualmente:

```
$>    rpm -ivh cyrus-sasl-gssapi-*.rpm
```

Per consentire che Kerberos si colleghi al server OpenLDAP generate un principal `ldap/earth.sample.com` e aggiungetelo nel `keytab`:

```
$> kadmin add -r ldap/earth.sample.com
$> ktutil get ldap/earth.sample.com
```

A questo punto deve esservi chiaro il seguente incoveniente: il server LDAP (slapd) gira solitamente come utente e gruppo `ldap`, mentre `keytab` può essere letto solo dall'utente `root`. Dunque o modificate la configurazione in modo che il server venga avviato come utente `root` o modificati i permessi di accesso rendendo `keytab` leggibile per il gruppo `ldap`.

Per lanciare slapd come root, editate il file /etc/sysconfig/openldap e disabilitate le variabili OPENLDAP_USER e OPENLDAP_GROUP inserendo un segno di commento all'inizio della riga.

Per rendere un file keytab leggibile per il gruppo ldap dovete procedere come riportato di seguito:

```
$> chgrp ldap /etc/krb5.keytab
$> chmod 640 /etc/krb5.keytab
```

Nessuna delle due soluzioni è una soluzione perfetta, però attualmente non è possibile configurare OpenLDAP in modo che utilizzi un proprio keytab.

Infine riavviate il server LDAP con rcldap restart.

Autenticazione Kerberos con LDAP

Adesso dovrebbe essere possibile eseguire applicazioni come ldapsearch automaticamente con l' autenticazione Kerberos.

```
$> ldapsearch -b ou=People,dc=suse,dc=de '(uid=newbie)'

SASL/GSSAPI authentication started SASL
SSF: 56
SASL installing layers
[...]

# newbie, People, suse.de
dn:uid=newbie,ou=People,dc=suse,dc=de
uid: newbie
cn: Olaf Kirch
```

Come potete vedere ldapsearch emette un messaggio indicando che ha lanciato l'autenticazione GSSAPI. Il seguente messaggio è un pò difficile da comprendere — il "Security Strenth Factor" (SSF) viene indicato con 56. (Il valore 56 è stato scelto arbitrariamente, probabilmente è stato scelto perché corrisponde ai 56 bit di una chiave di cifratura DES). In poche parole queste righe indicano che l'autenticazione GSSAPI è riuscita e che la connessione LDAP avviene in modo cifrato.

Non bisogna mai dimenticare che l'autenticazione Kerberos è sempre un processo bidirezionale, cioè non dovete autenticarvi solamente voi di fronte al server LDAP — anche il server dovrà farlo nei vostri confronti. Dunque potrete essere sicuri di comunicare con il server LDAP con il quale intendete comunicare, e non invece con un finto server dietro cui si cela un aggressore.

Per il caso sia possibile utilizzare diversi meccanismi SASL, con l' opzione `-Y GSSAPI` forzate ldapsearch ad utilizzare GSSAPI.

Autenticazione Kerberos e controllo di accesso LDAP

Nella sezione precedente abbiamo indicato come autenticarsi con successo sul server LDAP. Adesso ogni utente dovrà avere la possibilità di modificare l'attributo della shell di login nei suoi dati utenti LDAP.

Partiamo dal presupposto che la registrazione LDAP dell'utente `joe` si trovi sotto `uid=joe,ou=people,dc=suse,dc=de`, in questo caso potete stabilire le seguenti regole di accesso nel file `/etc/openldap/slapd.conf`:

```
# This is required for things to work _at all_
access to dn.base="" by * read
# Let each user change their login shell
access to dn="*,ou=people,dc=suse,dc=de" attrs=loginShell
       by self write
# Every user can read everything
access to *
       by users read
```

Con la seconda istruzione si permette ad utenti autenticati l'accesso in scrittura sull'attributo `loginShell` della vostra registrazione LDAP. La terza istruzione concede l'accesso in lettura alla completa directory di LDAP a tutti gli utenti autenticati.

Come fa il server LDAP a sapere che `joe@SAMPLE.COM` di Kerberos è l'equivalente del DN (*distinguished name*) LDAP `uid=joe,ou=people,dc=suse,dc=de`? Ciò viene stabilito manualmente tramite i valori della direttiva `saslExpr`. Aggiungete a `slapd.conf` per esempio:

```
saslRegexp
uid=(.*),cn=GSSAPI,cn=auth
uid=$1,ou=people,dc=example,dc=com
```

Per comprendere questo meccanismo dovete sapere che OpenLDAP crea un DN, quando SASL autentica un utente. Questo DN è composto dal nome consegnato da SASL, ad esempio `joe`, ed il tipo di autenticazione SASL (`GSSAPI`). In questo caso il risultato sarebbe `uid=joe,cn=GSSAPI,cn=auth`.

Se è configurato `saslRegexp`, il server LDAP controllerà il DN ricavato dall'informazione SASL con il primo argomento come espressione regolare. Se l'espressione regolare è quella giusta, il nome viene sostituito attraverso il secondo argomento della istruzione `saslRegexp`. I segnaposto (`$1`) vengono sostituiti da un espressione parziale che viene ricavata tramite l'espressione `(.*)`.

Chiaramente è possibile applicare degli schemi ancora più complessi. Se avete una struttura complessa di directory o il nome dell'utente nello schema da voi utilizzato non è parte del DN, potete utilizzare delle espressioni di ricerca che assegnano il DN SASL al DN dell'utente.

19.5 La sicurezza è una questione di fiducia

19.5.1 Concetti fondamentali

Una delle principali caratteristiche di un sistema Linux/Unix consiste nel fatto che diversi utenti possano lavorare contemporaneamente sul medesimo sistema (multi user e multitasking). Il sistema operativo offre inoltre trasparenza da un punto di vista della rete, di modo che gli utenti spesso non sanno se i file o le applicazioni con cui lavorano si trovano sul computer locale o vi accedono tramite la rete.

Per permettere a più utenti di lavorare su un sistema, i loro dati devono poter essere gestiti separatamente. È anche una questione di sicurezza e tutela della privacy. La sicurezza dei dati era importantissima 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 del manuale SuSE 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 sarà solo difficile accedere ai dati sul disco in caso di un difetto dell'hardware, ma anche e in particolar modo se vi è il sospetto che qualcuno abbia rovistato e magari manipolato in modo non autorizzato i nostri dati.

19.5.2 Sicurezza locale e sicurezza della rete

L'accesso ai dati avviene in modi diversi:

- parlando con qualcuno che disponga delle informazioni che si vorrebbero conoscere o che abbia accesso a determinati dati di un computer,
- direttamente dalla console di un computer (accesso fisico),
- tramite un'interfaccia seriale oppure
- tramite rete.

In tutti questi casi, dovrebbe esserci una costante: prima di ricevere l' accesso ai dati o alle risorse, l'utente dovrebbe e deve autenticarsi di fronte al sistema. Per un server web chiaramente le cose cambiano, comunque sicuramente non volete che il 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 e dell'intero sistema (compreso naturalmente il backup) - questo vale anche per il cavo di rete o la connessione di rete. 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.

Le interfacce seriali con terminali seriali sono ancora diffusi, ma non vengono quasi più installati su nuove postazioni di lavoro. In relazione al tipo

di accesso, il terminale seriale rappresenta un caso speciale: non si tratta di un'interfaccia rete, poiché per la comunicazione fra i singoli host non viene usato alcun protocollo di rete. Come mezzo di trasmissione per caratteri semplici, 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 registrarne il flusso di dati. Quello che è possibile con una stampante, è possibile anche con altri mezzi.

Dal momento che l'apertura di file su un computer sottosta a diverse restrizioni d'accesso rispetto all'accesso via rete ad un servizio di un computer, 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 dalla localizzazione fisica del computer. Noi partiamo dal presupposto che il vostro computer sia ubicato in modo da soddisfare i vostri criteri di sicurezza. Finché parliamo di sicurezza locale, bisogna anche distinguere i singoli utenti, in modo che nessun utente sia in grado di usare i permessi o l'identità di un altro. 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 confronta la password immessa con quella archiviata. Altrimenti, se venisse rubato il file con tutte le password, tutti gli account del sistema sarebbero compromessi. Linux salva invece 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, cosa che assicurano i cosiddetti algoritmi a trappola, che funzionano solo in una direzione. Un aggressore che sia riuscito ad impadronirsi della password cifrata non potrà semplicemente a sua volta ricalcolare la password dall'algoritmo per avere la password in chiaro, ma dovrà provare tutte le combinazioni di lettere possibili, finché non trovi quella che coincide con la vostra. 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 che l'algoritmo usato era molto lento e necessitava 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 di oggi non devono essere visibili ad ogni utente (per un utente normale, `/etc/shadow` non è leggibile) e le password non devono essere facili da indovinare – per il caso che, a causa di un errore, le password diventino visibili. Camuffare una password come Fantasia in 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, da cui verrebbe fuori 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 BIOS, ma esclusivamente dal disco rigido, impostazione che va fatta nel BIOS.

Generalmente, i sistemi Linux vengono inizializzati con un boot loader che permette di passare opzioni supplementari al kernel da avviare. Per quello che riguarda la sicurezza, tali opzioni sono molto critiche, perché il kernel non funziona solo con diritti root, ma assegna fin dall'inizio i diritti root. Se usate LILO come boot loader potete impedire ciò impostando un'ulteriore password in `/boot/grub/menu.lst` (vedi 7 a pagina 177).

Permessi di accesso

Qui vale il principio: lavorare sempre con i minori privileggi possibili. Non è assolutamente necessario leggere o scrivere una e- mail come root. Se il programma e-mail (MUA = Mail User Agent) con il quale lavorate 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 ridurre quanto più possibile i danni.

I singoli diritti dei più di 200.000 file di una distribuzione di SUSE sono stati assegnati in modo molto accurato. L'amministratore di un sistema dovrebbe installare software o file supplementari solo con la massima cura e

fare particolarmente attenzione all'assegnazione dei permessi sui file. Amministratori esperti e coscienziosi, quando usano il comando `ls`, aggiungono sempre l'opzione `-l` per avere un elenco dettagliato dei file assieme ai pemessi 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 i suoi permessi. Questo tipo di attacchi vengono chiamati "uova del cuccù", perché 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.

I sistemi di SUSE dispongono dei file `permissions`, `permissions.easy`, `permissions.secure` e `permissions.paranoid` che si trovano nella directory `/etc`. Qui vengono stabiliti i permessi paritcolari come p.es. directory con accesso in scrittura per tutti (world writable) o setuser-ID-bit per file, cioè il programma non viene eseguito coi diritti del proprietario del processo che lo ha iniziato, ma coi diritto del proprietario del file che è generalmente `root`). L'amministratore ha a disposizione il file `/etc/permissions.local` in cui può fissare 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 con YaST sotto 'Sicurezza'. Per ulteriori informazioni leggete il file `/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 stanno o stavano in un modo o nell'altro sotto la sfera di influenza di 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, che i dati non vengano scritti in aree della memoria troppo piccole e che i dati attraversano il programma e le interfacce definite in modo consistente.

Si ha un buffer overflow se, quando si scrive su un'area del buffer, senza badare alla dimensione effettiva del buffer. Potrebbe essere che i file (provenienti dall'utente) abbiano bisogno di più spazio di quello disponibile nel buffer: a causa di questo sfondamento dei limiti del buffer, può accadere che un programma, sulla base dei soli dati che deve elaborare, esegua sequenze di programmi che si trovano sotto l'influenza dell'utente e non del programmatore. Questo è un grave errore, specialmente se il programma

viene eseguito con diritti speciali (vedi sezione 19.5.2 a pagina 519). I format string bug funzionano un pò diversamente, ma anche queste utilizzano le immissioni dell'utente per fuorviare il programma.

Questi errori di programmazione vengono normalmente sfruttati da programmi che vengono eseguiti con privilegi alti, cioè programmi setuid e setgid. Potete quindi proteggere il vostro sistema e voi stessi da tali errori, togliendo dai programmi particolari diritti di esecuzione. Anche qui vale il principio dei minori diritti possibili (vd. paragrafo 19.5.2 a pagina 519).

Poiché i buffer overflow e format string bug sono degli errori nel modo di processare i dati degli utenti, questo tipo di bug può essere sfruttato non solo se si ha già accesso ad un login locale: molti degli errori conosciuti, possono venire sfruttati anche tramite un collegamento di rete. Per questo, buffer overflow e format string bug non si lasciano classificare nettamente come attinenti ai soli computer locali o alla rete.

Virus

Esistono virus anche per Linux! I virus conosciuti sono stati scritti dai loro autori come Proof-of-Concept, come prova dunque che il programma funziona. 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 p.es. il Master-Boot- Record e questo ospite deve 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 tale virus. Se, invece, vi attenete alla regola dei minori privilegi possibili, sarà difficile contaggiare il vostro sistema Linux con un virus. Inoltre, non dovreste mai eseguire sconsideratamente un programma preso da Internet e 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

Nella sicurezza locale, si tratta di separare nettamente gli utenti che condividono un computer, ed in particolar modo l'utente `root`. Per quando riguarda la sicurezza della rete è invece l'intero sistema che va protetto contro attacchi provenienti dalla rete. L'autenticazione dell'utente durante il login attraverso nome di login e password sono parte del concetto della sicurezza locale. Nel caso di il login tramite una connessione via rete bisogna differenziare 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 X11, il sistema windowing dei sistemi UNIX. Voi potete fare il login su un computer remoto ed inizializzare lì un programma che verrà visualizzato tramite la rete sul vostro computer.

Se un X-client deve venire visualizzato sul nostro X-server attraverso la rete, il server deve proteggere da accessi illeciti le risorse che amministra (il display). Concretamente significa che il programma del client deve ricevere dei diritti. Su X-Windows, questo avviene in due modi: controllo degli accessi basato su host e 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 nella mini-banca dati che si trova sul 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 al X-server esattamente come qualcuno che rubi l'indirizzo IP. Per questo qui non vogliamo approfondire questo metodo. La pagina di manuale di `xhost` vi fornirà maggiori dettagli sul funzionamento (e contiene anche questo avviso!).

Con l'accesso di controllo basato sui cookie viene usata, come mezzo di riconoscimento simile ad una password, una stringa nota solo al X-server e 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 la rinominate, non siete più in grado di aprire delle finestre di nuovi X-client. Nella pagina di manuale

di `Xsecurity` (`man Xsecurity`) troverete maggiori informazioni sugli aspetti di sicurezza di X-Windows.

`ssh` (secure shell) è in grado (tramite un collegamento di rete completamente cifrato) di creare in modo trasparente, cioè non direttamente visibile per l'utente, il collegamento ad un X-server: qui si parla di X11-forwarding. Sul lato server, viene simulato un X-server e nella shell sull'host remoto viene impostata la variabile DISPLAY.

Attenzione

Se siete del parere che il computer sul quale fate il login non sia sicuro, non create alcun collegamento X Windows. Con l'X11-forwarding attivato, potrebbero collegarsi al vostro X-server, tramite il vostro collegamento ssh, anche aggressori e origliare alla vostra tastiera.

Attenzione

Buffer overflow e format string bugs

Quanto detto nella sezione sicurezza locale su buffer overflow e format string vale anche per la distinzione in locale e remoto per gli aspetti relativi alla sicurezza della rete. Come anche nella variante locale di questo errore di programmazione, i buffer overflow portano quasi sempre ad avere i permessi `root` per i servizi della rete. Altrimenti, l'aggressore potrebbe procurarsi l'accesso ad un account locale (non privilegiato) tramite cui sfruttare altre falle nella sicurezza (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 cioè che sfruttano lacune rilevate di recente. Anche chi non conosca i dettagli esatti di questa lacuna, è in grado di trarrne di sfruttarle. Con l'andare degli anni, si è appurato che la libera disponibilità degli exploitcodes ha aumentato in generale la sicurezza dei sistemi operativi; la cosa dipende certamente dal fatto che i produttori di sistemi operativi sono stati costretti ad eliminare i bug nel loro software. Poichè con il software libero, il codice sorgente è a disposizione di tutti (il box SUSE Linux contiene tutti i sorgenti disponibili), ognuno che trova una lacuna con exploitcode, può anche fare una proposta 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 so-

vraccarico del sistema bombardandolo con pacchetti insensati o sfruttando cosiddetti remote buffer overflow.

Con un attacco DoS spesso si intende bloccare un servizio. La non disponibilità di un servizio può però avere conseguenze che vanno ben oltre. Si veda man in the middle: sniffing, tcp connection hijacking, spoofing e DNS poisoning.

man in the middle: sniffing, tcp connection hijacking, spoofing

In generale vale: 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 accetta il collegamento e, affinché la vittima non si accorga di nulla, crea egli stesso un collegamento con il sistema meta. La vittima, senza saperlo, ha aperto un collegamento di rete con il computer sbagliato, visto che questi si spaccia per il computer meta. L'attacco man in the middle più semplice è rappresentato da uno sniffer. Esso origlia ai collegamenti di rete che gli vengono fatti passare 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 TCP, l'aggressore deve analizzare per un pò di tempo i pacchetti che gli passano davanti. Quando assume il ruolo della meta del collegamento, la vittima lo nota solo perché il collegamento viene terminato perché non valido.

L'aggressore sfrutta soprattutto quei protocolli non protetti, non cifrati per l'hijacking e nei quali l'autenticazione avviene all'inizio del collegamento. Per Spoofing si intende l'invio di pacchetti con i dati mittente modificati, si tratta principalmente dell'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 possibilità di attacco appaiono solo in combinazione con un DoS. Se c'è la possibilità di staccare repentinamente un computer dalla rete (anche se solo per breve tempo), la cosa influenza favorevolmente un attacco attivo, poiché non si aspettano più alcuni disturbi.

DNS poisoning

L'aggressore cerca, con i pacchetti di risposta DNS falsificati (spoofed) di avvelenare *poisoning* la cache di un server DNS cosicché questi li inoltra ad una vittima che li richiede. Per indurre il server DNS ad accettare le informazioni alterate, di solito l'aggressore deve ricevere ed analizzare alcuni

pacchetti del server. Poichè molti server, sulla base del loro indirizzo IP e del loro nome host, hanno degli host classificati come affidabili, un tale attacco (nonostante la complessità) può portare entro pochissimo tempo al risultato desiderato. La premessa è una buona conoscenza del rapporto di fiducia fra questi computer. Dal punto di vista di colui che sferra l'accatto, un DoS come si deve che blocca un server DNS i cui dati devono venire falsificati, nella maggior parte dei casi non è evitabile.

Per evitare tutto questo si consiglia una collegamento criptato che può verificare l'identità della meta del collegamento.

Vermi informatici

I vermi vengono spesso comparati ai virus. Vi è tuttavia una notevole differenza: un verme non deve contagiare alcun programma ospite ed è tagliato per diffondersi rapidamente nella rete. I vermi conosciuti come Ramen, Lion o Adore sfruttano lacune di sicurezza ben conosciute di programmi di server come `bind8` o `lprNG`. È relativamente semplice proteggersi dai vermi, perché 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 sui propri sistemi tutte le più recenti security update.

19.5.3 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 la veloce integrazione di pacchetti di update annunciati 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.suse.de/security` seguendo i link. `suse-security-announce@suse.de` è la prima fonte di informazione per i pacchetti update rifornita continuamente con le ultime novità dal security-team.

La mailing list `suse-security@suse.de` è un foro di discussione molto informativo per il campo della sicurezza. Potete registrarvi a questa lista, sulla stessa URL di `suse-security-announce@suse.de`.

Una delle mailing list sulla sicurezza più conosciute nel mondo è `bugtraq@securityfocus.com` che consigliamo vivamente. Su `http://www.securityfocus.com` troverete ulteriori informazioni.

Ecco alcune utili regole di base:

- Lavorate il meno possibile come `root`, secondo il principio: per ogni compito, servitevi dei minori privileggi 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) è lo standard, evitate `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.e. `bind`, `sendmail`, `ssh`). Lo stesso vale per software che ha solo un'importanza locale per la sicurezza.
- Ottimizzate i permessi di accesso ai file critici in termini di sicurezza: fatelo adattando alle vostre necessità il file `/etc/permissions` di vostra scelta. Un programma setuid che non possiede più un setuid-bit, forse non sarà in grado di assolvere al suo compito, ma almeno non è più un problema di sicurezza. Idem per i world writable file e le world writable directory, ovvero file e directory a cui possono accedere in scrittura tutti.
- Disattivate ogni servizio di rete non strettamente necessario sul vostro server. Ciò rende sicuro il vostro sistema ed impedisce che i vostri utenti si abituino ad un servizio che non avete attivato intenzionalmente (legacy problem). Con il programma `netstat`, potete trovare porte aperte (con lo stato socket LISTEN). Come opzioni possono venire usate `netstat -ap` o `netstat -anp`. Con l'opzione `-p` vedete con quale nome il processo occupa la porta.

  Confrontate i risultati che avete con un port scan del vostro sistema eseguito dall'esterno; 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, poiché la cosa potrebbe venire scambiata per un tentativo di attacco. Ricordate di eseguire uno 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` e cifrare la banca dati per protegger-

la 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 hanno una firma gpg. La chiave che usiamo 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 pacchetto.rpm` mostra se la somma di controllo e la firma del pacchetto (non installare!) sono esatte. La chiave si trova sul primo CD o DVD di SUSE LINUX 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 ricerchi delle registrazioni strane nei vostri file di log. Questo è un compito tutt'altro che triviale, poiché solo voi sapete cosa sia strano o meno.

- 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 `tcpd(8)` e `hosts_access` (`man tcpd`, `man hosts_access`) troverete ulteriori informazioni su `tcp_wrappern`.

- In aggiunta a `tcpd` (tcp_wrapper) potreste usare il SuSEfirewall.

- Meglio esagerare in questi casi: ricordate che un comunicazione ricevuta due volte è meglio di una comunicazione mai ricevuta. Vale anche per la comunicazione tra colleghi di lavoro.

19.5.4 Rivelazione dei 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`. Aggiungete un'esatta descrizione del problema assieme al numero della versione del pacchetto usato. Cercheremo di rispondervi il più presto possibile. Se possibile, crittografate la vostra e-mail in pgp. La nostra chiave pgp 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.suse.de/security`.

Parte V

Appendixes

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.

Glossario

Meta-dati La struttura interna del file system che 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, data 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.

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.

Nota

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.

Nota

Ext2

Ext2 risale ai principi 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 esso ha 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 resi consistenti, 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 occupa una quantità notevolmente inferiore di spazio 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.

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 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 raggruppati in una transaction e 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 verificarsi che vecchi dati dopo un crash e ripristino ricompaiano nei file, mentre è garantita l'integrità interna del file system. Se non avete cambiato impostazioni, Ext3 viene inizializzato nel modo `data=ordered`.

Nota

Convertire un file system Ext2 in Ext3

Creare il journal: immettete `tune2fs -j root`. tune2fs crea il journal Ext3 con i parametri standard. Se volete determinare voi stessi la dimensione e su quale dispositivo il journal debba essere generato, immettete invece `tune2fs -J` accompagnato dai parametri `size=` e `device=`. Per ulteriori informazioni su tune2fs consultate la relativa pagina di manuale.

Stabilire il tipo di file system in `/etc/fstab`
Affinché il sistema rilevi e riconosca il file system Ext3 come tale, aprite il file `/etc/fstab` e modificate il tipo di file system della partizione interessata da `ext2` a `ext3`. Dopo il prossimo reboot del sistema la vostra modifica verrà applicata.

Nota

ReiserFS

Una delle funzionalità principali del kernel - ReiserFS - era ufficialmente disponibile a partire da SUSE LINUX 6.4 sotto forma di una patch di kernel per il kernel di SuSE 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. L'unica nota dolente: ReiserFS si concentra più sui metadati tralasciando i dati in sè. Le future versioni di ReiserFS conterranno il data-journaling (sia dati-meta che i dati concreti verranno scritti nel Journal) nonché accessi in scrittura ordinati (vedi `data=ordered` sotto Ext3). 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 a unità da 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. 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.

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 (throughput), visto che in questo ambito quello che conta è in prima linea è la prestazione. 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 la ricostruzione. 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 adatta 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.

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, al passo coi tempi viste le 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 su cui posa il 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, fino ad un certo grado, 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 *allocation* bipartendo il processo. Una transazione "in sospeso" 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.

Ulteriori file system supportati

La tabella A.1 elenca ulteriori file system supportati da Linux. Essi vengono supportati per garantire la compatibilità e lo scambio di dati tra diversi media o diversi sistemi operativi.

Tabella A.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.
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.e. 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.

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 più grandi 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 A.2 vi offre una rassegna delle attuali restrizioni per file Linux e file system per il kernel 2.4x.

Tabella A.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 3.5	2^{32} (4 GB)	2^{44} (16 TB)
ReiserFS 3.6 (sotto Linux 2.4)	2^{60} (1 EB)	2^{44} (16 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)

Nota

Limiti del kernel Linux

La tabella indica i limiti del on-disk format. La dimensione massima di un file e di un file system che viene processata correttamente dal sottosta - per il Kernel 2.4.x - alle seguenti restrizioni:

- *Sistemi a 32 bit:* File e block device non possono superare i 2 TB (2^{41} byte). Comunque tramite i LVM è possibile combinare diversi block device per potere gestire file system che superano i 2 TB.
- *Sistemi a 64 bit:* File e block device possono raggiungere i 8 EB (2^{63} byte) se l'hardware lo supporta.

Nota

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 *IBM developerWorks* riguardo ai file system di Linux si trova all'indirizzo :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

Le Access Control List in Linux

Questo capitolo vi 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 oggetti di file system tramite le ACL (*Access Control List*) ed i vantaggi che ne derivano.

Perché utilizzare le ACL?

Nota

POSIX ACLs

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/`

Nota

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

maggiori informazioni, consultate il *Manuale dell'utente* nella sezione *Utenti e diritti di accesso*.

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 progredite gli amministratori di sistema hanno dovuto escogitare una serie di espedienti per aggirare le restrizioni del 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 a livello della applicazione per implementare complessi modelli di permessi di accesso.

Quando si sostituisce un server Windows con uno Linux si apprezzeranno i vantaggi insiti nelle 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. Sul lato server le ACL possono essere modificate tramite getfacl e setfacl.

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). Nel*Manuale dell'utente* troverete una introduzione al concetto dell'utente in Linux, più precisamente nella sezione *Utenti e diritti di accesso*.

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 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 (vedi la tabella B.1), una designazione per l'utente o il gruppo a cui si riferisce la registrazione ed i permessi. Per alcuni tipi di registrazione non si immettete la designazione del gruppo o dell'utente.

Utilizzare le ACL

Nel seguente paragrafo vi mostriamo la struttura basilare delle ACL e le loro diverse varianti. Il nesso tra le ACL ed il modello d'assegnazione dei permessi tradizionale nel file system Linux verrà brevemente esposto anche sulla base di diversi grafici. In due esempi vi mostreremo come creare da voi delle ACL e come badare alla correttezza della sintassi. Infine vi mostriamo secondo quale schema il sistema operativo analizza le ACL.

Struttura delle registrazioni ACL

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*. La tabella B.1 riassume i diversi tipi di registrazioni ACL disponibili.

Tabella B.1: *Rassegna: tipi di registrazione ACL*

Tipo	Forma del testo
owner	`user::rwx`
named user	`user:name:rwx`
owning group	`group::rwx`

named group	`group:name:rwx`
mask	`mask::rwx`
other	`other::rwx`

I permessi stabiliti sotto *owner* ed *other* valgono sempre. Fatta eccezione per *mask* tutte le altre registrazioni, (ovvero *named user*, *owning group* e *named group*) possono essere rese effettive o mascherate. I permessi sono effettivi se sono stati impostati sia in una delle registrazioni sovramenzionate che nella maschera. I permessi impostati solo nella maschera o presenti solo nella registrazione in sé non sono validi. Con il seguente esempio cerchiamo di chiarire questo concetto (vedi la tabella B.2):

Tabella B.2: *Mascheramento dei permessi di accesso*

Tipo	**Forma del testo**	**Permessi**
named user	`user:jane:r-x`	`r-x`
mask	`mask::rw-`	`rw-`
	Permessi effettivi:	`r--`

Le registrazioni ACL ed i bit dei permessi

Le due figure illustrano il caso di una ACL minima ed una estesa (vedi la fig. B.1 a fronte e B.2 nella pagina successiva). 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* varia:

- Nel caso di una ACL minima — ovvero senza registrazione *mask* — i permessi *group class* vengono assegnati alla registrazione ACL *owning group* (vedi la fig. B.1 a fronte).
- Nel caso di ACL estese — dunque con la registrazione *mask* — i permessi *group class* vengono assegnati alla registrazione *mask* (vd. la fig. B.2 nella pagina successiva).

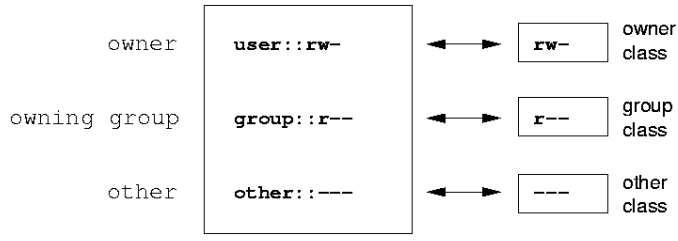

Figura B.1: *ACL minima: registrazioni ACL vs. bit dei permessi*

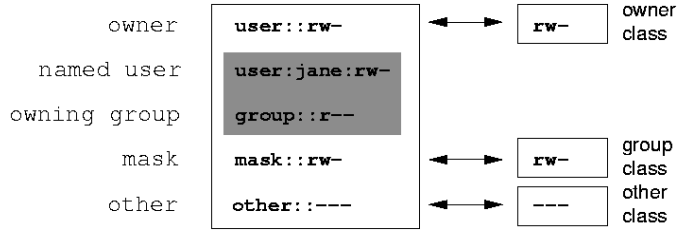

Figura B.2: *ACL estese: registrazioni ACL vs. bit dei permessi*

Grazie a questo tipo di assegnazione viene garantito che le applicazioni con e sprovviste di supporto per le ACL possano interagire senza difficoltà. 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 qui o non sono stati impostati nella ACL o non sono effettivi. Se si apportono delle modifiche ai bit dei permessi questo si rispecchia chiaramente anche nelle corrispondenti ACL e viceversa.

Una directory con ACL di accesso

I seguenti tre passi riportati nell'esempio vi permetteranno di lavorare con le ACL:

- Creare un oggetto di file system (nel nostro esempio una directory)
- Modificare l'ACL

- Utilizzare le maschere

1. Prima di creare una directory, il comando `umask` vi permette di stabilire a priori quali diritti di accesso mascherare:

   ```
   umask 027
   ```

   Con questo comando 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`).

   ```
   mkdir mydir
   ```

   Viene creata la directory `mydir/` con i permessi stabiliti con `umask`. Immettendo

   ```
   ls -dl mydir

   drwxr-x--- ... tux progetto3 ... mydir
   ```

   potete verificare se i permessi sono stati assegnati correttamente.

2. Dopo esservi informati sullo stato originario della ACL, aggiungetevi rispettivamente una nuova registrazione d'utente e di gruppo.

   ```
   getfacl mydir

   # file: mydir
   # owner: tux
   # group: progetto3
   user::rwx
   group::r-x
   other::---
   ```

   L'output di `getfacl` rispecchia esattamente la correlazione tra i bit dei permessi e le registrazioni ACL descritta nel paragrafo B a pagina 546. 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 `jane` ed ad un ulteriore gruppo `djungle` i permessi di lettura, scrittura ed esecuzione.

```
setfacl -m user:jane:rwx,group:djungle: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: progetto3
user::rwx
user:jane:rwx
group::r-x
group:djungle:rwx
mask::rwx
other::---
```

Oltre alle immissioni fatte da voi per l'utente `jane` ed il gruppo `djungle` 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, almeno ché 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 registrazione `mask`.

```
ls -dl mydir

drwxrwx---+ ... tux progetto3 ... mydir
```

In aggiunta nella prima colonna vi è un `+`, il segno per una ACL *estesa*.

3. In accordo con l'output del comando `ls` i permessi per la registrazione *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: `progetto3`) 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` (vedi la tabella B.2 a pagina 546). 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*.

```
chmod g-w mydir
ls -dl mydir

drwxr-x---+ ... tux progetto3 ... mydir

getfacl mydir

# file: mydir
# owner: tux
# group: progetto3
user::rwx
user:jane:rwx          # effective: r-x
group::r-x
group:djungle: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. Più chiaro risulta ciò 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`:

```
chmod g+w mydir
ls -dl mydir

drwxrwx---+ ... tux progetto3 ... mydir

getfacl mydir

# file: mydir
# owner: tux
# group: progetto3
user::rwx
```

```
user:jane:rwx
group::r-x
group:djungle:rwx
mask::rwx
other::---
```

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 gli 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

I permessi di accesso di una ACL di default vengono trasmessi ai propri sotto-oggetti principalmente in due modi:

- Una sottodirectory eredita l'ACL di default della directory superiore sia come propria ACl di default che ACL di accesso.
- Un file ereditata 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` ed dei permessi stabiliti nella ACL di default e quindi assegnati all'oggetto. `umask` in questo caso non viene considerato.

ACL di default nella prassi

Nel paragrafo seguente vi indicheremo come:

- Creare l'ACL di default per una directory esistente
- Creare una sottodirectory in una directory con ACL di default

- Creare un file in una directory con ACL di default

1. Aggiungete alla directory che avete creato prima `mydir/` una ACL di default:

   ```
   $> setfacl -d -m group:djungle: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: progetto3
   user::rwx
   user:jane:rwx
   group::r-x
   group:djungle:rwx
   mask::rwx
   other::---
   default:user::rwx
   default:group::r-x
   default:group:djungle:r-x
   default:mask::r-x
   default:other::---
   ```

   `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 riguardo l'ACL di default avete passato al comando `setfacl` solamente la registrazione per il gruppo `djungle`, `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: progetto3
user::rwx
group::r-x
group:djungle:r-x
mask::r-x
other::---
default:user::rwx
default:group::r-x
default:group:djungle:r-x
default:mask::r-x
default:other::---
```

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 anche 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/`:

```
touch mydir/myfile
ls -l mydir/myfile

-rw-r-----+ ... tux progetto3 ... mydir/myfile

$> getfacl mydir/myfile

# file: mydir/myfile
# owner: tux
# group: progetto3
user::rw-
group::r-x          # effective:r--
group:djungle: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, almeno ché `umask` o l'ACL di default non preveda altre restrizioni (vedi il paragrafo B a pagina 551).

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 registrazione *mask* in modo che vengano mascherati i bit dei permessi non impostati tramite `mode`.

In tal maniera si assicura che per esempio un compiler possa interagire senza difficoltà alcuna con le ACL. Potete creare dei file con permessi di accesso limitati ed contrassegnarli in seguito come eseguibili. `mask` fa sì che gli utenti e i gruppi ottengano anche i permessi concessi loro nella ACL di default.

Analisi di una ACL

Dopo aver compreso l'utilizzo dei tool principali di configurazione per le ACL introduciamo ora brevemente l'algoritmo di analisi che viene applicato ad ogni processo o applicazione prima di ottenere il permesso di accesso all'oggetto protetto da una ACL.

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 registrazione che più si adatta si regola quindi l'accesso.

Le cose si complicano un pò quando un processo appartiene a più di un gruppo, dunque quando teoreticamente anche più registrazioni *group* potrebbero essere quelle adatte. Tra le registrazioni adatte con i permessi richiesti viene selezionata una a caso. Infatti per il risultato finale "Accesso consentito" non fa differenza quale registrazione è stata scelta. Se nessuna registrazione *group* adatta ha i permessi corretti, è di nuovo una registrazione a caso che procura il risultato finale che in questo caso sarà "Accesso negato".

Supporto da parte degli applicativi

Come descritto nei paragrafi precedenti le ACL consentono di realizzare scenari per la concessione dei permessi di accesso davvero complessi all'altezza anche delle più recenti applicazioni. Il modello dei permessi tradizionale e le ACL si lasciano coniugare eccellentemente.

Però purtroppo alcune importanti applicazioni non supportano le ACL. In particolar modo in ambito delle applicazione di back-up - fatta eccezio-

ne per star - non vi sono dei programmi che mantengono le ACL anche a back-up avvenuto.

I comandi principali che riguardano i file come (`cp`, `mv`, `ls`, ...) supportano le ACL. 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, almeno ché l'editor non supporti le ACL.

Nota

Ulteriori informazioni

Informazioni dettagliate sulle ACL si trovano ai seguenti indirizzi: `http://sdb.suse.de/en/sdb/html/81_acl.html` `http://acl.bestbits.at/` e nelle pagine di manuale di `getfacl` la `acl` e la `setfacl`.

Nota

Manual-Page 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 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 system tree (--rebuild-tree). Normally you only need this option if the --check option reports "corruption that can be fixed with --fix-fixable". This includes: zeroing invalid data-block pointers, correcting st_size and st_blocks for directories, and deleting invalid directory entries.

--rebuild-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 discovered byte. This implies that holes at the end of a file will be removed. File sizes that are smaller than the offset of the last discovered byte are corrected by --fix-fixable.

--logfile file, -l file
This option causes reiserfsck to report any corruption it finds to the specified log file rather than stderr.

--nolog, -n
This option prevents reiserfsck from reporting any kinds of corruption.

--quiet, -q
This option prevents reiserfsck from reporting its rate of progress.

--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)
```

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 (vedi `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.

Nota

Questa traduzione non è un surrogato con validità legale per la versione originale in inglese!

Nota

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 2 nella pagina precedente

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 saran-

no 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.

Bibliografia

[1] *SUSE LINUX* (*Manuale dell'utente*). SUSE, 2. Edizione ©2003 .

[2] EDWARD C. BAILEY. *Maximum RPM*. ©1997 . ISBN 1-888172-78-9.

[3] BRYAN COSTALES, ERIC ALLMAN, NEIL RICKERT. *sendmail*. ©1993 . ISBN 1-56592-056-2.

[4] WERNER ALMESBERGER. *LILO User's guide*. `file:///usr/share/doc/lilo/user.dvi`.

[5] OLAF KIRCH. *LINUX Network Administrator's Guide*. ©1995 . ISBN 1-56592-087-2.

[6] SEBASTIAN HETZE, DIRK HOHNDEL, MARTIN MÜLLER, OLAF KIRCH. *Linux Anwenderhandbuch*. 6. Edizione ©1996 . ISBN 3-929764-05-9.

[7] SIMON GARFINKEL, GENE SPAFFORD. *Practical UNIX Security*. ©1993 . ISBN 0-937175-72-2.

[8] CRAIG HUNT. *TCP/IP Network Administration*. ©1995 . ISBN 3-930673-02-9.

[9] TIM O'REILLY, GRACE TODINO. *Managing UUCP and Usenet*. ©1992 . ISBN 0-937175-93-5.

[10] MATT WELSH. *Linux Installation and Getting Started*. 2. Edizione ©1994 . ISBN 3-930419-03-3.

[11] LINDA LAMB. *Learning the vi Editor*. ©1990 . ISBN 0-937175-67-6.

[12] MATT WELSH, LARS KAUFMAN. *Running Linux*. ©1995 O'Reilly. ISBN 1-56592-100-3.

[13] WILLIAM R. CHESWICK, STEVEN M. BELLOVIN. *Firewalls und Sicherheit im Internet*. ©1996 Addison Wesley. ISBN 3-89319-875-x.

[14] BRENT CHAPMAN, ELISABETH D. ZWICKY. *Einrichten von Internet Firewalls* (*Sicherheit im Internet gewährleisten*). ©1996 O'Reilly. ISBN 3-930673312.

[15] BRIAN TUNG. *Kerberos: A Network Authentication System*. ©1999 Fischer-TB. Verlag. ISBN 0-201-37924-4.

[16] CHIN FANG, BOB CROSSON, ERIC S. RAYMOND. *The Hitchhiker's Guide to X386/XFree86 Video Timing (or, Tweaking your Monitor for Fun and Profit)*. ©1993 .

Indice analitico

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Y