SuSE Linux

Manuale di amministrazione

6. Edizione 2004

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

autori: Frank Bodammer, Stefan Dirsch, Olaf Donjak, Torsten Duwe, Roman Drahtmüller, Thorsten Dubiel, Karl Eichwalder, Thomas Fehr, Stefan Fent, Werner Fink, Kurt, Garloff, Carsten Groß, Andreas Grünbacher, Franz Hassels, Andreas Jaeger, Klaus Kämpf, Hubert Mantel, Anas Nashif, Johannes Meixner, Lars Müller, Matthias Nagorni, Peter Pöml, Siegfried Olschner, Heiko Rommel, Marcus Schaefer, Nikolaus Schüler, Klaus Singvogel, Hendrik Vogelsang, Klaus G. Wagner, Christian Zoz
traduttori: Gaetano Lazzara, Barbara Improta Mann
redazione: Jörg Arndt, Antje Faber, Berthold Gunreben, Roland Haidl, Jana Jaeger, Edith Parzefall, Peter Reinhart, Thomas Rölz, Marc Rührschneck, Thomas Schraitle, Rebecca Walter
formato: Manuela Piotrowski, Thomas Schraitle
composizione: LaTeX

Questo manuale è stato stampato su carta sbiancata senza cloro.

Indice

II Configurazione 65

Prefazione

Il presente *Manuale d'amministrazione* vi illustrerà i principali aspetti di natura tecnica di SuSE Linux e tratterà i dettagli che riguardano l'installazione, l'amministrazione di sistema e la configurazione di speciali componenti del sistema. Inoltre vi presenteremo i concetti teorici che stanno alla base delle peculiarità di Linux ed in particolar modo di SuSE Linux. Faremo luce per esempio sul sistema X-Window, concetto di boot, processo di stampa e kernel Linux.

Le spiccate attitudini di Linux per l'utilizzo nella rete sono sempre state uno dei maggiori punti di forza di Linux, per questo abbiamo dedicato gran parte del manuale alla teoria, all'impostazione ed all'amministrazione di reti e dei suoi svariati servizi. Tratteremo dettagliatamente i diversi protocolli, il routing, l'NFS e NIS, reti eterogenee con Samba e Netatalk nonché i proxy. Il manuale si conclude con un capitolo dedicato al tema della sicurezza delle reti.

Vedrete che SuSE Linux, partendo dall'idea dell'open source, per il suo concetto di boot, facilità con la quale si lascia installare, e soprattutto per sua la stabilità e sicurezza che offre in tema di networking nonché la flessibilità dell'ambiente X11, è semplicemente il sistema operativo superiore!

A sistema installato avrete a vostra disposizione inoltre la versione digitale dei manuali di SuSE Linux, che troverete nel SuSE Help Center di SuSE Linux.

Novità del manuale di amministrazione

Segue un elenco delle novità e modifiche di questo manuale rispetto alla versione precedente:

- La sezione dedicata a GRUB nel capitolo sul boot loader è stata ristrutturata e sono stati aggiunti ulteriori dettagli (cfr. sezione *Boot con GRUB* a pagina 77).
- Il capitolo dedicato alla stampa è stato rielaborato (cfr. sezione *Stampare nella rete TCP/IP* a pagina 191).
- Il capitolo dedicato all'audio è stato spostato nel *Manuale dell'utente*.
- Il capitolo sui portatili è stato arricchito di una serie di dettagli su SCPM e power management (cfr. capitolo *Notebook – PCMCIA, APM, IrDA e SCPM* a pagina 213).
- Il capitolo introduttivo su IPv6 è stato completamente rielaborato (cfr. la sezione *IPv6 – l'Internet di prossima generazione* a pagina 322).
- Al capitolo sul Domain Name System sono state aggiunte le sezioni che trattano la sicurezza delle transazioni, l'aggiornamento dei file zona e DNSSEC (cfr. sezione *DNS – Domain Name System* a pagina 344).
- Il manuale è stato aggiornato in tanti punti in base alle novità di SuSE Linux 9.0.
- In più troverete:
  - Un capitolo dedicato al tema SuSE Linux su AMD64 (cfr. capitolo *SuSE Linux su sistemi AMD64* a pagina 253)
  - Un'introduzione dettagliata su LDAP (cfr. sezione *LDAP – Un servizio directory* a pagina 356)
  - Un capitolo sui principi di XNTP (cfr. sezione *Sincronizzare l'orario con xntp* a pagina 395)
  - Un capitolo introduttivo vertente sul server web Apache (cfr. capitolo *Il server web Apache* a pagina 397)

Convenzioni tipografiche

Nel presente manuale vengono utilizzate le seguenti convenzioni tipografiche:

Contrassegno	Significato
YaST	indica il nome del programma
`/etc/passwd`	indica il file o una directory
⟨*segnaposto*⟩	la sequenza di caratteri `segnaposto` (incl. la parentesi graffa) è da sostituire con il valore effettivo
`PATH`	una variabile di ambiente con il nome `PATH`
`192.168.1.2`	il valore di una variabile
`ls`	l'indicazione di un comando da immettere
`user`	l'indicazione di un utente
`terra:~ # ls`	immissione di `ls` nella shell dell'utente `root` nella directory home sul computer "terra"
`tux@terra:~ > ls`	immissione di `ls` nella shell dell'utente `tux` (nome ufficiale del Pinguino Linux) nella directory home sul computer "terra"
`C:\> fdisk`	prompt di DOS con l'immissione del comando `fdisk`
Alt	un tasto da premere; tasti da premere l'uno dopo l'altro sono separati da uno spazio
Ctrl + Alt + Canc	i tasti da premere contemporaneamente sono collegati da un `'+'`
"Permission denied"	avviso di sistema
'Aggiornare il sistema'	voci di menu, bottoni
"Modo DMA"	convenzioni, definizioni di nomi, cosiddetto...

Allori

Elencare tutti coloro che hanno contribuito alla riuscita di questa distribuzione riempirebbe le pagine di un libro. Ringraziamo tutti coloro che con il loro impegno indefesso hanno fatto sì che anche questa volta possiamo presentarvi un eccellente SuSE Linux che supera tutte le altre versioni presentate in precedenza.

É l'impegno volontario degli sviluppatori di 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 applicare numerosi adattamenti.

In questo capitolo troverete una descrizione delle diverse possibilità di installazione, per esempio l'installazione nel modo testuale con YaST ed indicazioni su come eseguire un'installazione da varie fonti 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

L'installazione in modo testo con YaST

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 X Window System non supporta la scheda grafica. Chiaramente anche i non-vedenti (che dipendono da un'interfaccia testuale) useranno il modo testo.

La schermata di avvio

Inserite il DVD oppure il CD 1 nel lettore e riavviate il computer. Se il sistema non esegue il boot, probabilmente dovrete cambiare la sequenza di caricamento nel BIOS del computer, impostandola su `CDROM,C,A`. Dopo un paio di secondi vedrete 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 il sistema a visualizzare il modo testo di YaST a tutto schermo. 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 testo se la scheda grafica crea delle difficoltà durante l'installazione. Infine premete ↵. 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 *Il CD-ROM ATAPI si inceppa durante la lettura* a pagina 24.

- Il CD 1, che contiene un kernel ottimizzato per i processori Pentium, non viene riconosciuto come mezzo di caricamento. Provate con un "dischetto di caricamento" o con il CD 2; cfr. le sezioni *Avvio dal dischetto (SYSLINUX)* a pagina 22 o *Caricare il sistema dal CD 2* a pagina 23.

- Nel caso di difficoltà dovute ad ACPI (ingl. *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 degli anni prima del 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://sdb.suse.de/en/sdb/html/81_acpi.html`

- Le schede grafiche del tipo FireGL 1, 2 o 3 non possono essere caricate nel modo grafico. In questo caso, l'installazione dovrà essere eseguita in ogni caso nel modo testo. Selezionate dunque (F2=Testo) nel menu di avvio.

- Selezionate 'Memory Test', per una verifica della memoria, in caso di difficoltà "inspiegabili" durante il caricamento del kernel o dell'installazione. Linux è molto esigente, in quanto ad hardware: la memoria ed il suo timing devono essere perfetti! Per maggiori approfondimenti, consultate:

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

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

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'. Con ↵ viene eseguito il comando selezionato.

Per una descrizione più dettagliata di linuxrc, consultate la sezione *linuxrc* a pagina 280 ss.

Impostazioni

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

Figura 1.1: *Scelta della lingua*

- Scegliete la lingua dell'installazione (ad esempio, 'Italiano') e confermate con ↵.
- Selezionate poi la mappatura della tastiera (per esempio '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).

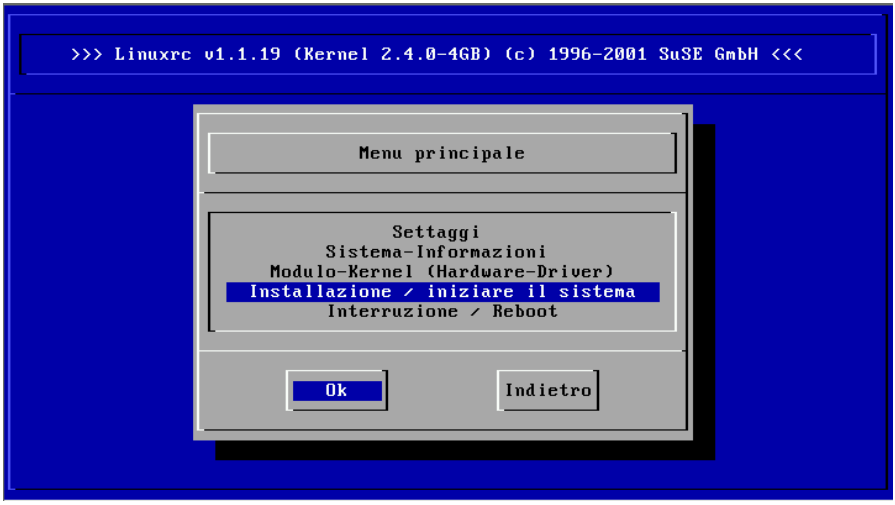


Figura 1.2: *Menu principale di linuxrc*

Questo menù vi offre le seguenti opzioni:

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

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

'Moduli del kernel (driver)' Se necessario, caricate i moduli corrispondenti all'hardware. In questo menù trovate anche una serie di file system (ReiserFS!) che potrete caricare in aggiunta.

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* AT-API. Alcuni driver adesso li trovate solo sotto forma di moduli che potrete caricare all'occorrenza (p.es. IDE) , altri sono stati aggiunti al kernel (per esempio USB, FireWire o file system).

Per sapere di più sul caricamento dei moduli, leggete la sezione *linuxrc* a pagina 280. 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 a pagina 17.

Uno o più file system – come ReiserFS o ext3.

Suggerimento

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.*Creare un dischetto di avvio sotto DOS* a pagina 20. Andate alla fine dell'elenco e selezionate la voce '-- Altri moduli --'; in questo caso, linuxrc vi chiederà il dischetto dei moduli.

Suggerimento

Avvia l'installazione

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

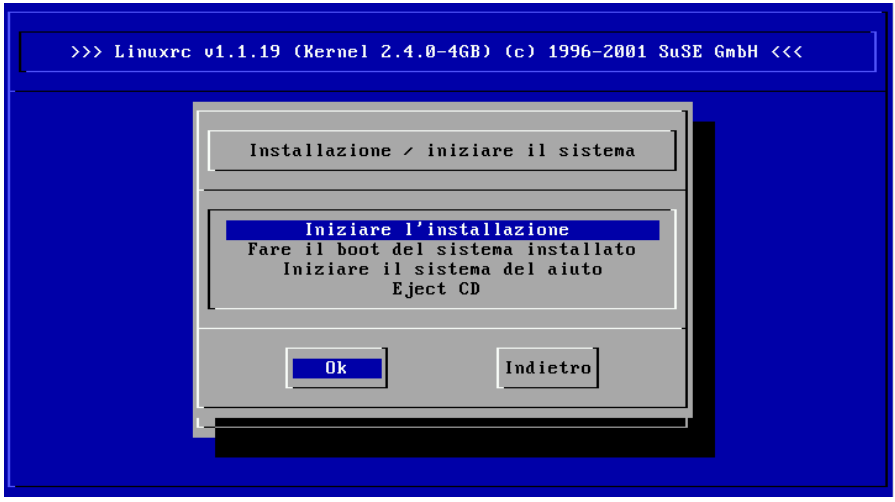


Figura 1.3: *Il menù d'installazione di linuxrc*

Potete scegliere tra i seguenti punti:

'Avvia installazione/update' Probabilmente, quello che siete in procinto di fare.

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

'Avvia sistema di salvataggio' Questa opzione vi aiuterà nel caso si verifichino dei problemi con il sistema da installare.

'Espelli CD' Per estrarre il CD per via elettronica.

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

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

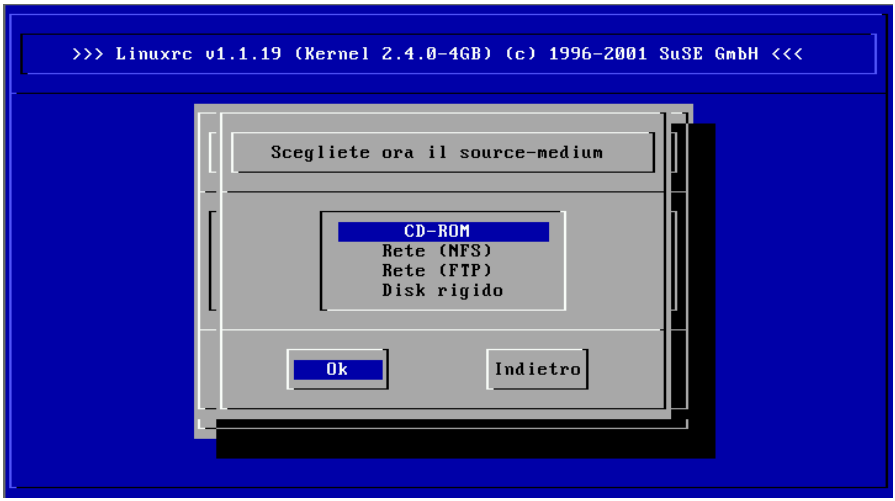


Figura 1.4: *Selezionare il mezzo sorgente su linuxrc*

Problemi possibili

- 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 *Il CD-ROM ATAPI si inceppa durante la lettura* a pagina 24.
- Eventualmente possono verificarsi delle difficoltà durante il caricamento dei dati nella ram-disk, in modo che non è possibile 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' su no. Tornate al menù principale e ricominciate l'installazione da capo.

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 possibilità per caricare di 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. [SuS03], 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 per OS/2 o Windows NT.

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 per esempio 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 . 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 sui diversi metodi per il boot, specialmente LILO e loadlin, nel capitolo 4 a pagina 73 ss.

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.

Disattiviare la schermata SuSE

In linea di massima avete tre possibilità:

- disattivare la schermata all'occorrenza immettendo sulla riga di comando:

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

  e il seguente comando per riattivarla:

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

- disattivare la schermata di default:

  Aggiungete un parametro del kernel `splash=0` alla configurazione del bootloader. Nel capitolo *Boot e boot manager* a pagina 73 troverete delle informazioni dettagliate. Se preferite comunque il modo testo, lo standard nella versioni precedenti, impostate `"vga=normal"` .

- disattivare la schermata per sempre:

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

Suggerimento

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!

Suggerimento

Installazioni particolari

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

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 per esempio con il seguente comando:

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

Cambiate in seguito il nome della directory (per esempio "CD1"):

```
terra:/ #  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 *NFS – file system dislocati* a pagina 385.

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 *Creare un dischetto di avvio sotto DOS* a pagina 20 e *Creare i dischetti di avvio in un sistema Unix-like* a pagina 21. 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 (per esempio `eepro100`).
5. Selezionate 'Carica driver del file system' e caricate i driver richiesti (per esempio `reiserfs`).
6. Selezionate 'Indietro' ed infine 'Avvia installazione / sistema'.
7. Selezionate 'Avvia installazione / update'.
8. Selezionate 'Rete' e poi come protocollo di rete per esempio `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 (per esempio `/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 [SuS03], 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.

Consigli e trucchetti

Creare un dischetto di avvio sotto DOS

Premesse

Vi serve un dischetto 3.5 pollici HD, ovvero ad alta densità, formattato e un lettore floppy 3.5 pollici 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; dopo 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 (ingl. *source*) e la destinazione (ingl. *destination*) del file da copiare. In questo esempio, si tratta del dischetto di caricamento appartenente al set di CD, la cui immagine si trova su 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.

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.

Procedete così per creare un dischetto di avvio:

1. Se dovete ancora formattare il dischetto:

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

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

   ```
   terra:~ #  mount -tiso9660 /dev/cdrom /media/cdrom
   ```

3. Andate nella directory boot sul CD:

   ```
   terra:~ #  cd /media/cdrom/boot
   ```

4. Ora create il dischetto di avvio con

   ```
   terra:~ #  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 stessi 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 *Compilare il kernel* a pagina 264):

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

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 *Creare un dischetto di avvio sotto DOS* a pagina 20 oppure *Creare i dischetti di avvio in un sistema Unix-like* nella pagina precedente.

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

- 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.

Suggerimento

Premendo (Shift) all'avvio di SYSLINUX, tutti questi processi verranno saltati.

Per il debug, aggiungete la riga

```
verbose 1
```

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

Suggerimento

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`

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).

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 sotto `http://cdb.suse.de/` 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 *Avvio dal dischetto (SYSLINUX)* a pagina 22. Prima di eseguire l'avvio dal dischetto accertatevi che gli dispositivi USB siano collegati e accesi.

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:

hd⟨*x*⟩=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 se siete in possesso di un CD-ROM drive ATAPI.

ide⟨*x*⟩=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.

Partizionare per esperti

Nel capitolo sulla installazione standard vengono trattate le possibilità di partizionamento del sistema. Questo paragrafo intende fornire solo 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.

Premettiamo subito che non c'è *un* metodo d'oro per tutti, bensì tanti metodi d'oro per ciascuno. Non preoccupatevi! In questo capitolo troverete schemi chiari che vi serviranno come punto di riferimento.

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)?

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; oggi chi compra un computer con meno di 64 MB di memoria, non ha buoni consiglieri. Ma ritorniamo alla

Installazione	Spazio richiesto
minima	180 MB fino a 400 MB
piccola	400 MB fino a 800 MB
media	800 MB fino a 4 GB
grande	4 GB fino a 8 GB

Tabella 1.1: *Esempi per la dimensione di installazioni*

suddetta affermazione. Il nostro obiettivo è quello di avere un computer che disponga di ca. 30/ 40 MB di memoria virtuale.

Con applicazioni moderne che richiedono molta memoria, bisogna correggere i valori "verso l'alto". Normalmente 128 MB di memoria virtuale dovrebbero essere sufficienti, ma qui è meglio non essere tirchi. Se si compila un kernel sotto X e si consultano le pagine d'aiuto con Netscape, mentre contemporaneamente sta girando Emacs, con 128 MB di memoria virtuale non rimangono più molte riserve.

Perciò come utente medio si è al sicuro con almeno 256 MB di memoria virtuale. Quello che non dovete assolutamente fare è: non dedicare alcun spazio alla memoria swap. Perfino su un computer con 256 MB RAM dovrebbe esserci un settore di swap; la ragione di ciò la vedrete nella sezione *Velocità del disco e la dimensione della memoria principale* a pagina 30.

Avete intenzione di far girare simulazioni elabortatissime e necessitate gigabyte di memoria? Se doveste avere dei dubbi sul fatto che Linux possa offrirvi una base sufficientemente solida per le vostre applicazioni, andate alla sezione *Impiego come server di calcolo* a pagina 28 (Campo d'impiego: server di calcolo).

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 della vostre necessità. Nella tabella 1.1 avete un sommario dei diversi volumi d'installazione per un sistema Linux.

Naturalmente i valori aumentano in base alla mole di dati aggiuntivi che volete salvare su hard disk.

Esempio: computer standard per postazione di lavoro (molto 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 1.5 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 152 GB, non esiste nessuno standard di partizionamento; vedi la sezione *Ottimizzazioni* nella pagina seguente.

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, directory degli utenti di una banca dati o di archivi vari. 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 su `/home`, se non tutti gli utenti si mettono a compilano 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 questo caso dividere `/home` su due dischi da 4 GB, poiché questi si possono dividere il carico di lavoro (e il tempo di accesso).

Suggerimento

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

Suggerimento

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.

Ottimizzazioni

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 (per esempio `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 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).

```
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
```

output 1: *Esempio di output del comando df*

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

```
root@terra:/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 la lettura/scrittura dei buffer interni 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 coi dati dell'hard disk. Per farlo Linux utilizza vari trucchetti, come p.e. "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 *Il comando free* a pagina 273.

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 nel capitolo *Partizionare per esperti* a pagina 25.

Nota

Di solito le partizioni vengono stabilite 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, dietro al bottone 'Esperti...', troverete un menù a tendina con i seguenti comandi:

Rileggi tabella di partizione Per rileggere le partizioni del vostro disco rigido. Questo comando vi serve, 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. Di far leggere il vecchio `fstab`, ne avrete bisogno se scegliete di non attualizzare, ma di reinstallare il vostro sistema. 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 sovrapporre la nuova tabella delle partizioni alla vecchia. Vi servirà nel caso in cui, ad esempio, vi sono dei problemi con label un pò particolari. Con questo metodo, tuttavia, perderete tutti i dati del disco rigido.

Logical Volume Manager (LVM)

Il Logical Volume Manager (LVM) vi permette di ripartire in modo flessibile lo spazio del vostro disco rigido per 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, in caso di necessità, possano essere creati dei volumi logici (LV). Il sistema operativo potrà poi ricorrere a questi ultimi, anzicché a delle partizioni fisiche.

Particolarità:

- Più dischi rigidi/partizioni possono essere riunite in un unica grande partizione.
- Se un LV si riempie (per esempio `/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 back-up 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 se ne possono avere fino a 256. 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 o un documento SuSE:

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

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, selezionate ‘Crea’ → ‘Non formattare’ e cliccate 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...’.

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).

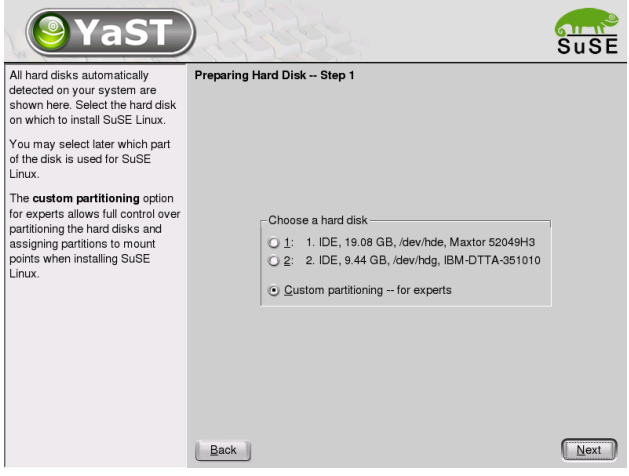


Figura 1.5: *YaST: attivare LVM durante l'installazione*

Suggerimento

Ripartizionare i Logical Volume

All'inizio dei PV vengono scritti delle informazioni sul 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 per esempio con il comando

```
dd if=/dev/zero of=/dev/sda2 bs=512 count=1
```

Suggerimento

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 seguite, e non sarà 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 appartenga ad un volume group attivato non potrà essere più modificato. Il kernel di Lin-

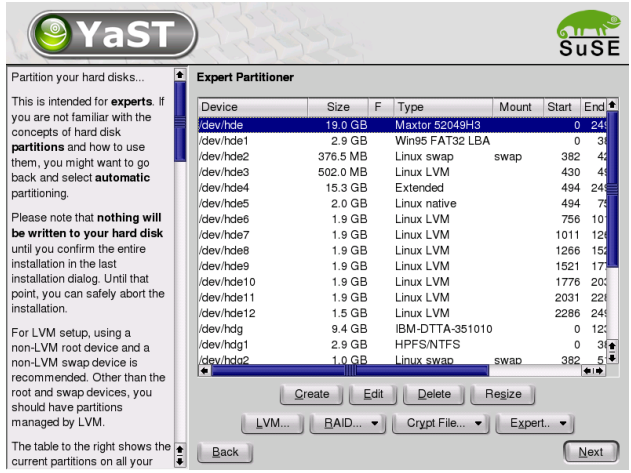


Figura 1.6: *YaST: il partizionatore*

ux si rifiuterà di leggere un partizionamento modificato, fintanto che anche una sola partizione 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 una tale partizione dalla lista e fatene un file system root facendo clic sul pulsante 'Modifica'.

Dato l'elevato grado di flessibilità dell' LVM, consigliamo di impostarvi tutti gli altri file system. 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 per il 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

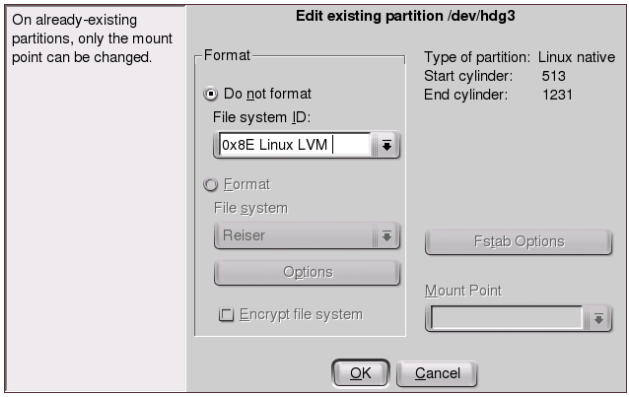


Figura 1.7: *YaST: creare una partizione*

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

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 sistema SuSE Linux normalmente installato, non è necessario creare più di un volume group. Una partizione assegnata ad un volume group viene anche definita Physical Volume (o più spesso: 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 lasciare inutilizzato una parte dello spazio della partizione. Prima di chiudere il dialogo, ad ogni volume group dovrà essere attribuito almeno un physical volume.

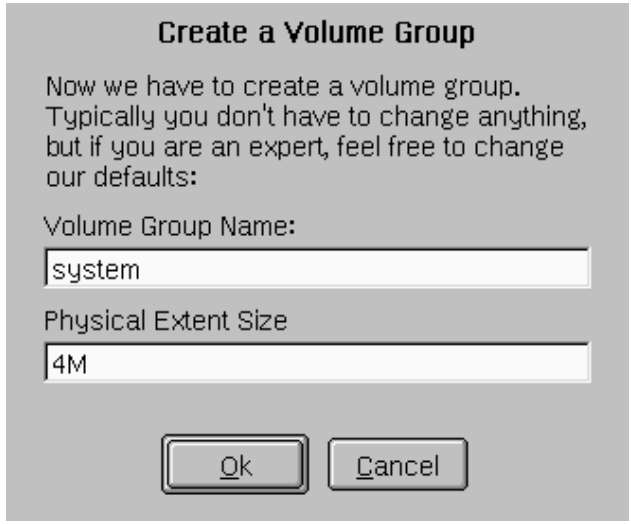


Figura 1.8: *YaST: creare un volume group*

Logical Volumes

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. Uno striping 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 (per esempio 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.

In caso abbiate già configurato 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:

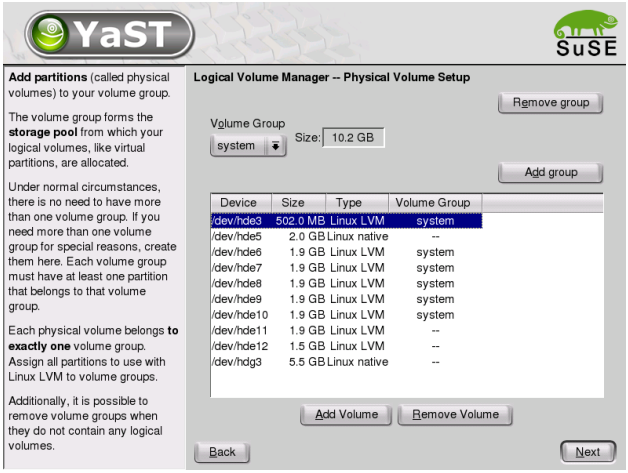


Figura 1.9: *YaST: lista delle partizioni*

dovrete crearne uno per ogni punto di mount (tramite il bottone 'Aggiungere') e determinarne l'estensione, il tipo di file system (per esempio reiserfs oppure ext2) ed il punto di mount (per esempio `/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 passare alla selezione del software, nel caso in cui vi troviate nel mezzo del processo di installazione

Attenzione

L'impiego di un LVM può comportare una serie di rischi, come la perdita dei dati. Possibili pericoli sono crolli di programma, caduta di corrente o comandi errati.

Create una copia di sicurezza dei vostri dati prima di usare l'LVM o di riconfigurazione dei volume – non lavorate mai senza un back-up!

Attenzione

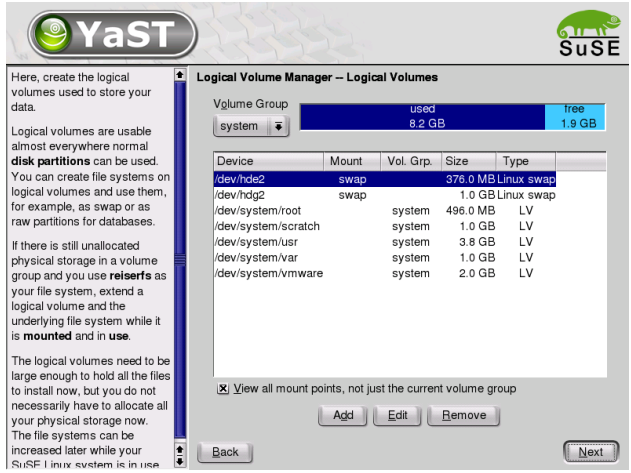


Figura 1.10: *YaST: amministrazione dei Logical Volume*

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 la fusione e l'indirizzamento dei dischi rigidi tramite 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'esecuzione 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.

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

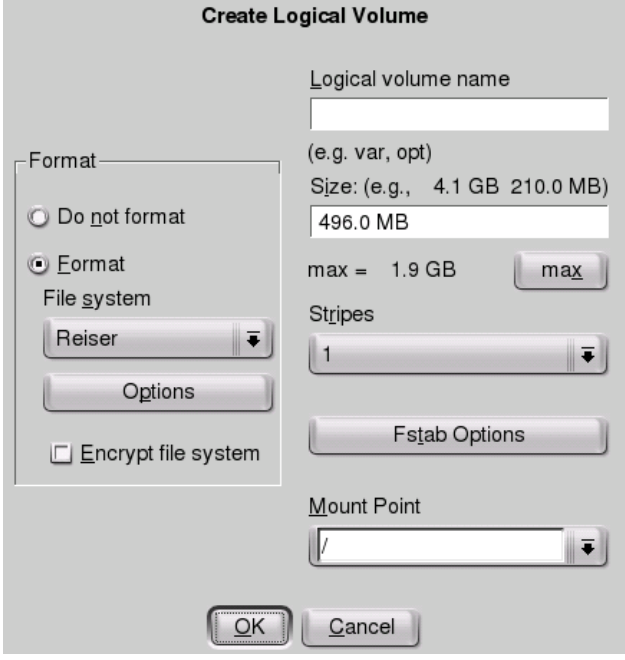


Figura 1.11: *YaST: creare logical volume*

uniscono 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 sarà distrutto e i vostri dati 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 doppiati 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 i dati.

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'.

Primo passo: partizionare

Per prima cosa, alla voce 'Impostazioni 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: normalmente, di esattamente due con RAID 1. 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.

Secondo 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 adattamento 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://www.LinuxDoc.org/HOWTO/Software-RAID-HOWTO.html`

o la mailing list di Linux RAID per esempio via:

- `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.

2

Aggiornare il sistema e amministrare i pacchetti

Aggiornare il sistema e amministrare i pacchetti

SuSE Linux vi offre la possibilità di attualizzare un sistema, senza doverlo re-installare. È possibile sia *attualizzare pacchetti di software singoli*, che *attualizzare l'intero sistema*.

I singoli pacchetti possono essere anche installati con il programma di gestione dei pacchetti rpm.

Attualizzare 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 prescelto e dalla versione da aggiornare a SuSE Linux.

Nota

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

Nota

Preparazione

Prima di iniziare l'aggiornamento, i vecchi file di configurazione dovrebbero essere copiati su un dispositivo a parte (streamer, hard disk estraibile, dischetto, 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 dell'utente sotto `/home` (le directory `HOME`). 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

```
terra:~ #  df /
```

scoprite il nome del dispositivo della vostra partizione root; nel caso dell'output 2 è `/dev/hda7` la partizione root da annotare.

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/hda1             1.9G  189M  1.7G  10% /dos
/dev/hda7             3.0G  1.1G  1.7G  38% /
/dev/hda5              15M  2.4M   12M  17% /boot
```

output 2: *Panoramica con df -h*

L'output mostra che la partizione `/dev/hda7` è ("montata") nel file system su `/`.

Problemi possibili

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

I controller della Promise I controller del 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 *La schermata di avvio* a pagina 8. Questo parametro dovrà anche essere inserito nella configurazione del boot, con YaST, se avete intenzione di usarlo a lungo; cfr. il capitolo*Installazione personalizzata, Il boot (Installazione del boot loader)* nel manuale [SuS03].

Attenzione

Spiegazione tecnica

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 il caricamento del sistema!

Attenzione

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 Promise diretto), 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.

L'update con YaST

Dopo i preparativi riportati nella sezione *Preparazione* 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 3. Se vi sono più partizioni, selezionate la partizione giusta e confermate la vostra selezione con 'Prossimo' (nell'esempio nella sezione *Preparazione* 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 di aggiungere nuovi ed importanti componenti di software al sistema ("modo upgrade"). Si consiglia di accettare quanto proposto (per esempio 'Sistema standard'). Delle eventuali incongruenze possono essere eliminate in un secondo momento ricorrendo a YaST.

L'update manuale

Aggiornare il sistema di base

Poiché, all'aggiornamento del sistema di base devono venire modificate anche le parti centrali del sistema (per esempio 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 *L'installazione in modo testo con YaST* a pagina 8 ss.:

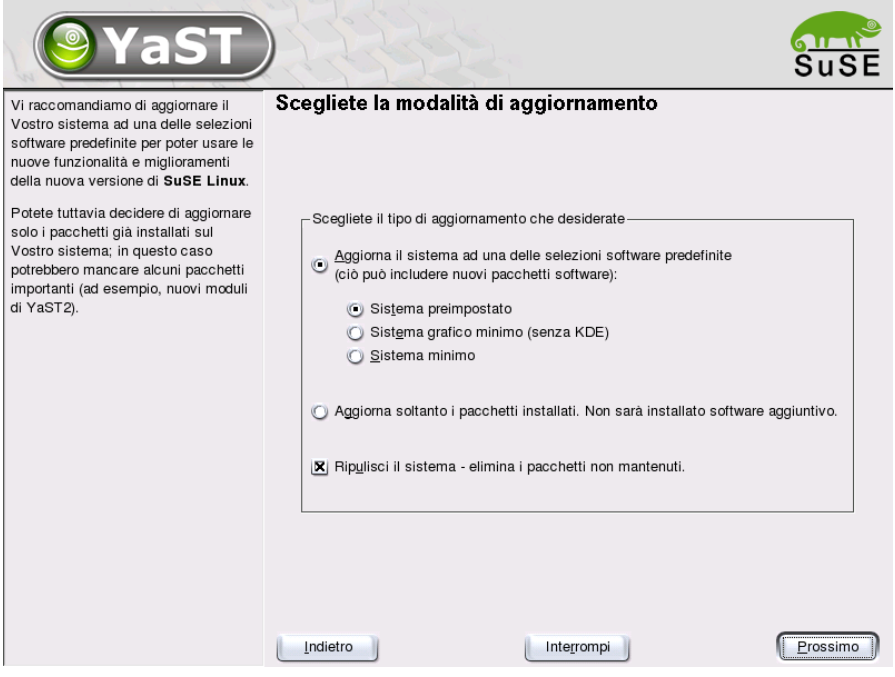


Figura 2.1: *Update del software*

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 *La base: linuxrc* a pagina 10 e la descrizione di linuxrc a pagina 282.

4. Una volta fatto ciò, si può passare, tramite i punti del menù 'Avvia installazione / sistema' → e 'Inizializza installazione/update', alla scelta del supporto di installazione. (vedi a pagina 284).

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'.

Alla fine, YaST cerca la partizione root e mostra il risultato. Selezionate o confermate una delle partizioni: indicate nell'elenco la vostra partizione root come descritto sopra (esempio: `/dev/sda3`). In questo modo, incaricate YaST di leggere la "vecchia" `fstab` che si trova su questa partizione. YaST analizzerà ed in seguito monterà i file system lì registrati.

Avrete poi la possibilità 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 siano stati modificati dall'ultima installazione. Poi, vengono archiviate vecchie versioni dei file di configurazione (che di solito hanno l'estensione `.rpmorig` o `.rpmsave`, cfr. sezione *Amministrare i pacchetti: installarli, aggiornarli e disinstallarli* a pagina 56); 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 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.

Suggerimento

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

Suggerimento

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
  ```

Attualizzare i 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.

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 dell'utente o dell'amministratore di sistema. L'elenco non è completo. In quel che segue, vi rimandiamo anche al corrispondente articolo della banca dati di supporto spesso abbreviata con SBD; gli articoli della SDB nel pacchetto `sdb_en`.

Appena rilevati, le difficoltà e le particolarità della rispettiva versione verranno pubblicati sul Server-WWW; cfr. i link riportati di seguito. Per importanti aggiornamenti di singoli pacchetti, visitate il sito `http://www.suse.de/de/support/download/updates/`.

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. *Creare un dischetto di avvio sotto DOS* a pagina 20 o *Creare i dischetti di avvio in un sistema Unix-like* a pagina 21.
- YaST 2 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 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. pacchetto `kbd`, pacchetto `isapnp`, pacchetto `lvm` ecc.); cfr. a pagina 302.
- Nell'ambito della rete sono vi sono stati una serie di cambiamenti; cfr. a riguardo la sezione *L'integrazione nella rete* a pagina 331
- Per amministrare i file di protocollo (ingl. *log file*), si usa il programma logrotate; `/etc/logfiles` non è più necessario; cfr. sezione *File di log – il pacchetto logrotate* a pagina 270.
- Il login di `root` tramite telnet o rlogin può essere impostato nei file su `/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.
- locatelocate, usato per trovare subito dei file, non appartiente più al software standard. Se necessario, installatelo in un secondo momento (pacchetto `find-locate`) e vedrete che, circa un quarto d'ora 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`.

Dalla versione 8.0 alla 8.1

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

- Modificare i nomi degli utenti e dei gruppi del sistema: per essere consistenti con UnitedLinux, 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 *Filesystem Hierarchy Standard (FHS)* a pagina 268):
  - Un'ambiente esempio per HTTPD (Apache) si genera sotto `/srv/httpd` (ex `/usr/local/httpd`).
  - Un'ambiente esempio per FTP si genera sotto `/srv/ftp` (ex `/usr/local/ftp`). É richiesto il pacchetto 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 per esempio `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 in 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 con YaST.

- Pacchetti che cambiano nome: `bzip` diventa `bzip2`.

- Pacchetti non più inclusi: `openldap`, utilizzate adesso `openldap2` e `sudo` al posto di `su1`.

Dalla versione 8.1 alla 8.2

Problemi e particolarità:
`http://sdb.suse.de/sdb/en/html/bugs82.html`.

- Supporto 3D per schede sonore nVidia (cambiamenti): gli rpm -Pakete `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 (pacchetto `openjade`) è ora il motore DSSSL che sostituisce jade (pacchetto `jade_dsl`) quando invocate db2x.sh (pacchetto `docbook-toys`). Per motivi di compatibilità i pacchetti sono disponibili anche senza il prefisso `'o'`.

  Se alcune applicazioni dipendono da file della directory `jade_dsl` dovrete adattare le applicazioni 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 il pacchetto `rzsz` il tool per la riga di comando `sx` continua a chiamarsi `s2x/ sgml2xml` oppure `osx`.

Dalla versione 8.2 alla 9.0

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

- 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`; `rpm` viene utilizzato come prima per installare, aggiornare e per richiste alla banca dati; cfr. la sezione 2.
- Per quel che riguarda il processo di *stampa* vi è il pacchetto `footmatic-filters`. Il contenuto è stato preso dal pacchetto `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 dipendo dal sistema di stampa (CUPS, LPRng). Il file di configurazione del pacchetto è `/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.

RPM – Il package-manager della distribuzione

SuSE Linux ricorre a RPM (`rpm`) (ingl. *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 (ingl. *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 *Linux Standard Base (LSB)* a pagina 268.

Suggerimento

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`: il pacchetto `alsa-devel`, il pacchetto `gimp-devel`, il pacchetto `kdelibs-devel` etc.

Suggerimento

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.

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 (per esempio `/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;. per esempio 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 *Inoltrare richieste* a pagina 61).

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 dipine 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 pac-

chetto 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 pagina di manuale di `rpm` (`man 1 rpm`) oppure nella pagina di manuale di `rpmbuild` (`man 1 rpmbuild`).

Inoltrare richieste

Con l'opzione `-q` (ingl. *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 *Inoltrare richieste* in questa pagina.

`-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

Tabella 2.1: *Le opzioni di richiesta più importanti (*`-q [-p]` *...* ⟨*pacchetto*⟩*)*

Il comando

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

elenca le informazioni nell'output 3 :

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

output 3: *rpm -q -i wget*

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. 1); il nome del file cercato è da indicare come parametro alla chiamata dello script.

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

file 1: *Script cerca-pacchetti*

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:

`5`	somma di controllo MD5
`S`	grandezza del file
`L`	link simbolico
`T`	ora della modifica
`D`	"major" e "minor" (ingl. *device number*)
`U`	utente (ingl. *user*)
`G`	gruppo (ingl. *group*)
`M`	modo (incl. diritti e tipo)

Tabella 2.2: *I controlli*

Nei file di configurazione viene emessa anche una `c`. Per esempio, nel caso sia stato modificato qualcosa in `/etc/wgetrc` del pacchetto `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.

Installare e compilare i pacchetti dei sorgenti dei pacchetti

Tutti i sorgenti (ingl. *sources*) di SuSE Linux terminano in `.src.rpm`, si tratta di "source-RPM".

Suggerimento

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*.

Suggerimento

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".0

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 (pacchetto `libc`, pacchetto `rpm`, pacchetto `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`.

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 pacchetto `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 di `build` (`man 1 build`).

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 professionisti 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.

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

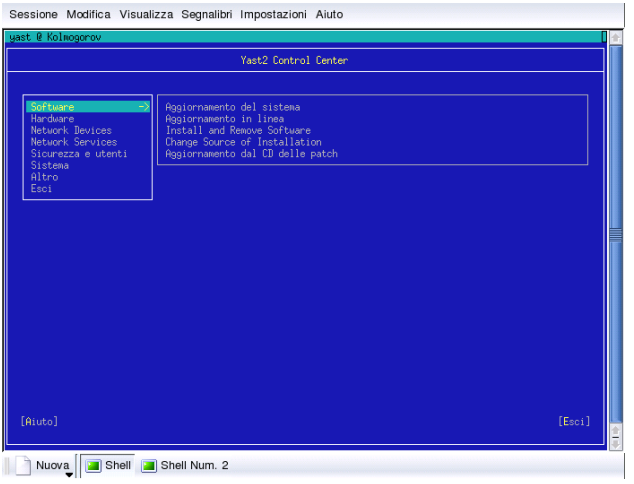


Figura 3.1: *La finestra principale di YaST-ncurses*

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 selzione che presentano una lettere di un colore diverso, giallo di default. Con la combinazione di (Alt) + (lettera gialla) potete selezionare il bottone direttamente senza dover ricorrere a (Tab).

Per uscire dal centro di controllo di YaST1 vi è il bottone 'Esci', oppure selezionate la sotto-voce'Esci' nella panoramica delle categorie e date (Enter).

Restrizioni riguardanti la combinazione dei tasti

Se sul vostro sistema con il 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 ⇑ 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, per esempio Esc + h al posto di Alt + h.

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

Restrizioni dei tasti funzione: Anche i tasti funzione sono già occupati (vd. sotto). 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.

Nel seguente paragrafo si parte dal presupposto, per maggior chiarezza, che le combinazioni con Alt funzionino.

Usare i moduli

Navigare tra i bottoni/liste di selezione: Per scorrere i bottoni e/o le liste di selezione usate rispettivamente i tasti Tab e Alt + Tab.

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, per esempio i singoli moduli di un gruppo di moduli nel centro di controllo.

Marcare bottoni e check box Per selezionare bottoni con una parentesi quadra vuota (check box) o con le parentesi tonde (radio bottoni) servitevi della barra spaziatrice o Enter. Per selezionare i bottoni nel margine inferiore dei singoli moduli premete Enter, quando sono già evidenziati (color verde), oppure in modo più veloce con la combinazione Alt + tasto_giallo (cfr. Fig. 3.2 nella pagina seguente).

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 (per esempio dettagli, informazioni, aggiungi, cancella...). In YaST con il tasto F1 vi potete fare indicare le funzioni dei tasti funzione.

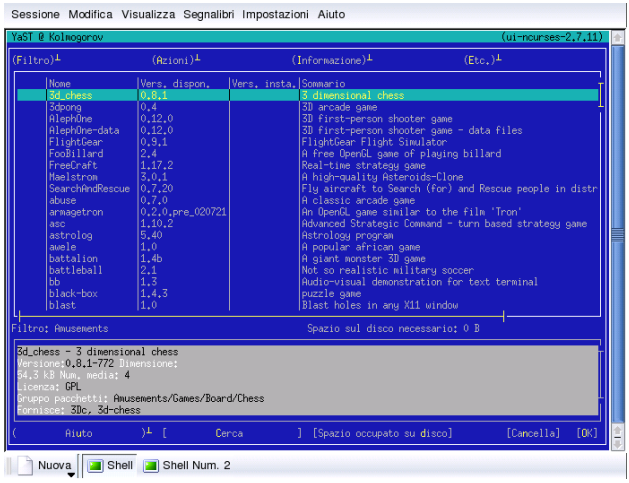


Figura 3.2: Il modulo per l'installazione del software

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 per esempio 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 `yast --list`.

YOU: YaST Online Update

Potete lanciare YOU anche dalla console; immettendo come `root`

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

scaricate la lista delle patch attuale e tutti i relativi .rpm dal primo server nella lista `/etc/suseservers`. Se vi interessano solo determinate patch, potete aggiungere delle opzioni.

Le opzioni possibili sono `security`, `recommended`, `document`, `YaST` ed `optional`. `security` scarica solo patch concernenti la sicurezza, `recommended` gli update consigliati da SuSE, `document` vi fornisce delle informazioni sulle patch o sul server FTP, `YaST` scarica solo patch di YaST e `optional` fornisce degli update non di primaria importanza.

Le informazioni sulle patch sono memorizzate sotto `/var/lib/YaST2/patches/<arch>/update/`$\langle X.Y \rangle$`/patches`. Possono essere letti solo da `root`. $\langle X.Y \rangle$ indica la versione di SuSE Linux. `<arch>` si riferisce alla architettura del sistema sul quale utilizzate SuSE Linux.

Il comando per scaricare le patch di sicurezza:

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

Ogni volta che immettete `.auto.get` normalmente la lista dei server FTP viene copiata sotto `/etc/suseservers`. Se non volete che ciò avvenga, dovete disabilitare questa funzione nel file `/etc/sysconfig/onlineupdate`.

```
YAST2_LOADFTPSERVER="yes"
```

va impostato da `yes` su `no`. Installate ora la patch con

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

Questo comando installa tutte le patch selezionate. Se volete installare solo un gruppo, potete utilizzare le stesse opzioni descritte per `.auto.get`.

Questo metodo ha il vantaggio che si lascia automatizzare. L'amministratore di sistema può scaricare i pacchetti per esempio durante la notte e installare quelli che necessità la mattina.

Il cron job per YOU

Visto che non tutti che vogliono/devono usare YOU, sanno anche come impostare un cron job, segue una breve descrizione del processo. In linea di massima esistono due possibilità per farlo, riportiamo di seguito quella più semplice:

1. Diventate root
2. Avviate l'editor per crontab con il comando `crontab -e`.
3. Premete la lettera `i` per la modalità di inserimento di vi
4. Inserite le seguenti righe:

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

   I primi 5 caratteri della seconda e terza riga vanno letti da sinistra a destra e stanno per: 13=minuti, 3=ore, *=giorno del mese, non fa differenza, *=mese dell'anno, non fa differenza, 0=domenica. Dunque il tutto significa che la prima registrazione inizializza il job di cron ogni domenica alle 3 e 13 di notte. La seconda dopo 40 minuti, alle 3 e 53. La riga `MAILTO=" "` impedisce che root riceva l'output di YaST-ncurses come e-mail e può essere naturalmente omessa.

   Attenzione

   Immettete dei vostri orari per i job di cron, però non quelli riportati nell'esempio, altrimenti, a quell'ora il server ftp risulta sovraccarico o si supera il numero massimo degli accessi contemporanei consentiti.

   Attenzione

5. Salvate il job di cron (premendo l'uno dopo l'altro) Esc `:wq` ed ↵ con Esc e `ZZ`.

Il demone di cron viene automaticamente riavviato e il vostro job di cron viene registrato nel file `/var/spool/cron/tabs/root`.

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 e il suo predecessore LILO.

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.

Dopo aver terminato il suo "controllo interno", il sistema può dedicarsi alla ricerca dell'hardware collegato. Informazioni riguardanti la data attuale, l'ora e le periferiche più importanti vengono lette dai valori CMOS (*CMOS setup*). Poiché a questo punto il primo hard disk e la sua geometria dovrebbero essere stati rilevati, si può cominciare con l'avvio del sistema operativo.

Per farlo, dal primo hard disk viene caricato in memoria 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.

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 *Partizionare per esperti* a pagina 25. Senza la tabella delle partizioni, non esistono neppure i file system, cioè 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.

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 formattate in DOS, Windows

o OS/2 (che contengono inoltre importanti dati di base 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 di avvio di sistema valido deve avere negli ultimi 2 byte lo stesso contrassegno "magico" dell'MBR (AA55).

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* (ingl. *bootable*), il che significa si deve cercare là il sistema da caricare. 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 (ingl. *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 95/98.

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.

Concetti di boot

Il più semplice "concetto di boot", riguarda un computer con un solo sistema operativo; per questo caso abbiamo già descritto i processi della fase di avvio. Questo processo vale anche per PC su cui gira solo Linux. Teoricamente allora si potrebbe rinunciare ad installare LILO, 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 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 to 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 dovete riavviare il computer. La premessa è comunque che il boot manager funzioni bene con i diversi sistemi operativi.

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 di Linux vi erano tanti file system 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.

Adesso spiegheremo come installare e configurare GRUB, seguirà l'illustrazione delle differenze rispetto a LILO che viene descritto nei suoi particolari in [Alm96]. Le istruzioni si trovano sotto: `/usr/share/doc/packages/lilo/user.dvi`. Potete visualizzare il documento allo schermo con applicazioni del tipo `xdvi` o stamparlo con il comando:
`lpr /usr/share/doc/packages/lilo/user.dvi`

Nota

Quando viene installato quale boot loader?

Se eseguite un aggiornamento da una vecchia versione di SuSE Linux che utilizza LILO, viene installato nuovamente LILO. Se eseguite una nuova installazione viene installato invece GRUB, almenoché la partizione root si trovi su uno dei seguenti sistemi Raid:

- Controller Raid che dipendono dalla CPU (come p.es. tanti controller Promise oppure Highpoint)
- Software-Raid
- LVM

Nota

Boot con GRUB

GRUB (ingl. *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 può accedere 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), motivo per cui modifiche apportate al file di configurazione di GRUB non significano più dover reinstallare il boot manager. All'avvio GRUB ricarica il file menu e i percorsi attuali e 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.

Il menu di boot di GRUB

Lo splash screen grafico con il menu di boot viene configurato tramite il file di configurazione di GRUB path/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 i file — utilizzate semplicemente YaST2 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 di una concatenazione con boot loader di altri sistemi operativi. Il comando è `chainloader` e l'argomento è di solito il blocco di boot di un'altra partizione nella *block notation* di GRUB, per esempio:

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

I nomi dei dispositivi in GRUB vengono spiegati nella sezione *Denominazioni dei dischi rigidi e partizioni* a fronte. 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 vi è in un `menu.lst` creato 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 *Esempio di un file menu* nella pagina successiva.

Denominazioni dei dischi rigidi e partizioni

GRUB utilizza una convenzione diversa per designare dischi rigidi e partizioni rispetto ai "soliti" dispositivi Linux (p.es. `/dev/hda1`). 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 *Il file device.map* a pagina 83.

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.

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

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 lasciate lo 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 badate che 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 interventi possibili.

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 esegue 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, dopo aver lasciato uno spazio, alla riga esistente.

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
```

Se al prossimo boot del sistema si dovessero verificare delle difficoltà, controllate la sequenza di boot e cambiatela se necessario tramite la GRUB shell. 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 delle modifiche apportate manualmente al file `device.map`, date il seguente comando per reinstallare GRUB:

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

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, per quel che riguarda i comandi che seguono.

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, quando Linux è in esecuzione. 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 entra in gioco l'algoritmo di correlazione. Il programma legge il file `device.map` composto da righe con un nome di dispositivo GRUB e un nome di dispositivo Linux ciascuna. Visto che la sequenza dei dischi rigidi IDE, SCSI e di altro tipo dipende da diversi fattori e Linux non può riconoscere la correlazione, vi è la possibilità di stabilire la sequenza in `device.map`. Se si verificano delle difficoltà durante il boot controllate se la sequenza in questo file corrisponde a quella del BIOS. Il file si trova nella directory GRUB `/boot/grub/`). Per maggiori dettagli vedi la sezione *Il file device.map* nella pagina precedente.

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:

- 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 è possibile immettere dei comandi GRUB in fase di boot solo dopo aver immesso (p) e la password. In questo caso continua ad essere consentito agli utenti di lanciare un sistema operativo dal menu di boot.

- Per escludere questa possibilità, 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

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". In questi casi utilizzate LILO o aggiornate eventualmente il BIOS.

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'`sdb.suse.de`, gli articoli sono tradotti tra l'altro anche in inglese.

Il boot con LILO

Il boot loader Linux LILO si installa nell'MBR. LILO ha accesso ad ambedue gli hard disk rilevati nella modalità reale e già a partire dalla sua installazione è in grado di trovare tutti i dati necessari riguardanti gli hard disk "raw" senza avere informazioni sul partizionamento; questo è il motivo per cui si può fare il boot dei sistemi operativi anche dal secondo hard disk. Contrariamente al processo di boot in DOS, vengono ignorate le registrazioni nella tabella delle partizioni.

La differenza principale rispetto al processo di boot di DOS consiste tuttavia nella possibilità di poter scegliere al boot tra i diversi sistemi operativi da caricare. Dopo che l' MBR è stato caricato nella memoria, viene avviato LILO; LILO presenta all'utente un elenco di sistemi preinstallati. All'avvio del sistema carica i settori di boot delle partizioni per poter avviare il sistema operativo da questa partizione, oppure carica il kernel di Linux ed avvia Linux. Inoltre consente di passare al kernel di Linux una riga di comando. Per motivi di sicurezza i servizi di LILO possono essere protetti parzialmente o completamente da una password.

I principi

Ecco le componenti coinvolte all'avvio del sistema con LILO:

- I *settori di boot di LILO* con una parte iniziale ("il primo livello") del codice LILO che attiva il LILO vero e proprio all'avvio del sistema.
- Il codice macchina di LILO, locazione standard: `/boot/boot-menu.b`
- Il *file mappa* (`/boot/map`), in cui al momento della sua installazione LILO registra dove trovare il kernel e altri dati necessari.
- Optional: il *file messaggio* `/boot/message`, che genera di default un selezione di boot LILO grafica.
- I diversi kernel di Linux e settori di boot da poter avviare conLILO .

Attenzione

Ogni accesso in scrittura (anche spostare un file) ad una di queste componenti, invalida il file mappa e rende perciò necessaria una *nuova installazione di LILO* (paragrafo *Installazione dopo aver modificato la configurazione* a pagina 92)! Questo riguarda particolarmente il passaggio ad un nuovo kernel Linux.

Attenzione

Il settore di boot di LILO può essere installato:

Su un *dischetto* Questo è il metodo più facile ma anche più lento per eseguire il boot con LILO. Selezionate questo metodo se non volete sovrascrivere il settore di boot esistente.

Nel *settore boot* di una partizione Linux primaria del primo hard disk Questa opzione non va a toccare l'MBR. Prima del boot questa partizione deve essere attivata con fdisk. Invocate come `root fdisk -s <partizione>` Apparirà il prompt di fdisk. `'m'` vi elenca le possibilità di inserimento, e con `'a'` potete rendere pronta per l'avvio la partizione indicata.

Nel *Master Boot Record* Questa opzione offre maggior flessibilità; inoltre è l'unica possibilità di caricare Linux dall'hard disk, se tutte le partizioni Linux si trovano sul secondo hard disk e sul primo non si ha nessuna partizione estesa. Se l'installazione non viene eseguita in modo adeguato, una modifica dell'MBR comporta anche certi rischi.

Se finora avete usato un *altro boot manager* ... e volete continuare a usarlo, ci sono, a seconda delle sue funzionalità, anche altre possibilità. Un caso molto comune: avete una partizione Linux primaria sul secondo hard disk da cui volete inizializzare Linux. L'altro boot manager sarebbe in grado di farlo tramite il settore di boot: potete rendere avviabile questa partizione, installando LILO nel suo settore di boot e dichiarando all'altro boot manager che essa è attiva.

Configurazione di LILO

LILO può essere adattato alle vostre richieste: in seguito spiegheremo le più importanti opzioni e il loro significato. Per una descrizione dettagliata vi rimandiamo a [Alm96].

La configurazione di LILO viene registrata nel file `/etc/lilo.conf`. Vi consigliamo di tenere pronto il file di configurazione utilizzato all'ultima installazione di LILO e di farne una copia di sicurezza prima di apportare delle modifiche. Le modifiche vengono applicate reinstallando LILO con l'ultima versione del file di configurazione (sezione *Installazione e disinstallazione di LILO* a pagina 92)!

La struttura del file lilo.conf

`/etc/lilo.conf` inizia con una *sezione di opzioni globali* (ingl. *global options section*) che contiene configurazioni generali, seguita da una o più *sezioni del sistema* (ingl. *image sections*) per i singoli sistemi operativi che devono venire inizializzati da LILO Ogni nuova sezione del sistema viene introdotta da una riga con l'opzione `image` o `other`.

L'ordine dei singoli sistemi operativi in `lilo.conf` è significativo solo per il fatto che *prima* viene caricato il sistema in cima alla lista, a meno che l'utente non esegua una scelta diversa – prima che scadi il tempo d'attesa prestabilito (vedi sotto: opzioni delay e timeout).

Il file *La struttura del file lilo.conf* in questa pagina mostra una configurazione esempio su un computer con Linux e DOS. Al boot avete la scelta tra un nuovo kernel (`/boot/vmlinuz`), un kernel Linux di ripiego (`/boot/vmlinuz.suse`), Windows su `/dev/hda1` ed il programma Memtest86.

```
### LILO global section
boot    = /dev/hda           # LILO installation target: MBR
backup  = /boot/MBR.hda.990428  # backup file for the old MBR
```

```
                                # 1999-04-28
vga     = normal              # normal text mode (80x25 chars)
read-only
menu-scheme = Wg:kw:Wg:Wg
lba32                         # Use BIOS to ignore
                              # 1024 cylinder limit
prompt
password = q99iwr4            # LILO password (example)
timeout = 80                  # Wait at prompt for 8 s before
                              # default is booted
message = /boot/message       # LILO's greeting

### LILO Linux section (default)
  image  = /boot/vmlinuz      # Default
  label  = linux
  root   = /dev/hda7          # Root partition for the kernel
  initrd = /boot/initrd

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

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

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

file 2: *Configurazione esempio in /etc/lilo.conf*

In `/etc/lilo.conf` tutto ciò che si trova tra un # e la fine della riga è un "commento". Viene completamente ignorato da LILO può essere usato per una migliore leggibilità. Ora osserviamo passo per passo le più importanti righe: le altre opzioni sono descritte in *La struttura del file lilo.conf* nella pagina precedente.

- **Sezione globale** (Parte sui parametri)
  - ▷ boot=⟨*dispositivo di boot*⟩

Dispositivo sul cui primo settore deve venire installato il settore boot di LILO (il target dell'installazione).
⟨*dispositivo di boot*⟩ può essere: un floppy drive (`/dev/fd0`), una partizione (p. e. `/dev/hdb3`), o un intero disco (p. e. `/dev/hda`), questo significa l'installazione nell'MBR.

Default: se mancano queste indicazioni, LILO viene installato sulla partizione root Linux attuale.

- ▷ lba32
  Questa opzione elude il limite dei 1024 cilindri di LILO. Naturalmente questo funziona solo se ciò viene supportato dal BIOS del vostro computer.

- ▷ prompt
  Forza la visualizzazione del prompt di LILO. L'impostazione di default è: niente prompt! (Vedi paragrafo *La struttura del file lilo.conf* a pagina 88, opzione delay.)
  È consigliabile nel caso che LILO debba avviare più di un sistema operativo. Si dovrebbe anche configurare l'opzione timeout per rendere possibile un reboot automatico nel caso non vi è alcuna immissione al prompt.

- ▷ timeout=⟨*decimi di secondo*⟩
  Pone un intervallo per la scelta del sistema da caricare e rende così possibile un avvio automatico, a meno chè non si effettui per tempo una selezione. ⟨*decimi di secondo*⟩: è il tempo a disposizione per effettuare una propria immissione, espresso in decimi di secondo. Se premete il tasto ⇑ questa funzione viene disabilitata e il computer attenderà una vostra immissione. Default: 80!

- **Sezione Linux**

  - ▷ image=⟨*immagine-del-kernel*⟩nopagebreak
    Qui deve trovarsi il nome dell'immagine del kernel da caricare, solitamente `/boot/vmlinuz`.

  - ▷ label=⟨*nome*⟩
    In `/etc/lilo.conf` un nome univoco, ma negli altri casi un nome che può essere assegnato liberamente al sistema (p.e. Linux). La lunghezza massima è di 15 caratteri: possibilmente solo lettere, cifre e underscore (carattere di sottolineatura) – niente spazi, caratteri speciali con accenti e simili. Le regole esatte per i caratteri consentiti si trovano in [Alm96], sezione 3.2.1. Default: il nome della immagine del kernel (p.es. `/boot/vmlinuz`).

Sotto questo nome, all'avvio del sistema, selezionate il sistema operativo da caricare. Se si hanno più sistemi operativi, è consigliabile creare un file messaggio con una precisa descrizione dei nomi e sistemi (vedi il paragrafo *La struttura del file lilo.conf* a pagina 88, opzione message.

- ▷ root=⟨*rootdevice*⟩
  Con questo LILO indica al kernel la partizione root (p.e. `/dev/hda2`) del sistema Linux. Consigliato per motivi di sicurezza! Se si tralascia questa opzione, il kernel prende la partizione root registrata in sè stesso ⟨*kernelimage*⟩.
- ▷ append=⟨*parametro*⟩
  Se in un secondo momento volete consegnare a LILO ulteriori opzioni di boot per il kernel, aggiungete a `lilo.conf` una riga con append all'inizio e dopo il carattere = immettete il rispettivo parametro tra virgolette e separato da uno spazio. Dopo questa modifica LILO va reinstallato come utente `root` con `lilo`, affinché le modifiche vengono rese effettive al prossimo boot.

- **Sezione di Linux** (Linux – Safe Settings)

  Se avete installato un kernel proprio, è sempre possibile ricorrere a questo kernel ed avviare il sistema.

  - ▷ optional
    Se viene cancellato `/boot/vmlinuz.shipped` (*NON* lo consigliamo!), all'installazione di LILO, questa sezione viene saltata senza comunicazione di errori.

- **Altro sistema**

  - ▷ other=⟨*partizione*⟩
    Con other vengono indicate a LILO le partizioni di avvio di altri sistemi per il boot (per esempio `/dev/hda1`).
  - ▷ label=⟨*name*⟩
    Date un nome a questo sistema; l 'impostazione di default – solo il nome del dispositivo della partizione – è poco indicativa.

- **Memtest** Qui è registrato solo il programma per la verifica della memoria.

In questa sezione si è parlato solo delle registrazioni principali in `/etc/lilo.conf`. Per ulteriori impostazioni, consultate la pagina di manuale di `lilo.conf` che potete visualizzare con `man lilo.conf`.

Installazione e disinstallazione di LILO

Attenzione

Prima di installare LILO, assicuratevi *in ogni caso* di poter caricare eventualmente gli altri sistemi operativi dal dischetto (non funziona con Windows XP/2000/NT)! In particolare serve fdisk. SuSE Linux può essere caricato eventualmente anche dal CD o DVD di installazione.

Attenzione

Installazione dopo aver modificato la configurazione

Se avete modificato le componenti di LILO o la configurazione in `/etc/lilo.conf`, dovete reinstallare LILO. Ciò avviene chiamando semplicemente il cosiddetto *map-installer* come `root`:

```
/sbin/lilo
```

Ecco cosa succede: LILO crea un backup del settore (di boot) di destinazione, vi scrive il suo "primo livello" e crea un nuovo file mappa (vedi paragrafo a pagina 86). Uno dopo l'altro, LILO comunica i sistemi installati – p.e. nel caso del nostro esempio di configurazione:

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

Dopo aver concluso l'installazione, si può riavviare il computer (come utente `root`):

```
shutdown -r now
```

Dopo che il BIOS ha eseguito il suo test del sistema, appare LILO con la sua richiesta d'immissione in cui potete indicare parametri per il kernel e potete scegliere la boot image. Con (Tab) si possono elencare le denominazioni delle configurazioni installate.

Rimuovere LILO

Per disinstallare GRUB oppure LILO, il settore di boot dove è stato installato il boot loader Linux (GRUB oppure LILO) viene sovrascritto con il contenuto precedente. Sotto Linux questo non rappresenta un problema, *sempre che ci sia* un

backup valido. Utilizzate il modulo boot loader di YaST per creare un backup dell' MBR originale e da ripristinare eventualmente nel menu del boot loader o per creare un MBR standard. Il modulo boot loader di YaST viene descritto nella parte dedicata alla installazione nel *Manuale dell'utente*.

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 "bombe ad orologeria", la cosa migliore è cancellarli subito!

Attenzione

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 toccano l'attuale tabella delle partizioni, almeno che l'MBR (vedi a pagina 74) 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* (ingl. *bootable*); le MBR-routine di DOS, Windows, OS/2 lo richiedono!

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 X 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.

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.

Caricare Linux dopo il ripristino dell'MBR

Dopo aver ripristinato l'MBR standard di Windows, potete impostare il boot loader Linux di vostra scelta per continuare ad utilizzare il sistema Linux installato.

GRUB

GRUB ripone un "stage1" nella partizione Linux anche nel caso di una installazione nell'MBR. Dopo il ripristino dell'MBR con YaST o tramite i tool offerti da Windows descritti sopra, marcate come attiva la partizione Linux ricorrendo a fdisk. Basta dare il comando `fdisk /dev/`⟨*`disco rigido`*⟩ come utente `root`. fdisk aspetta una vostra immissione. Con 'm' ottenute una rassegna delle possibilità a vostra disposizione, con 'a' modificate la tabella delle partizioni in modo che proprio una partizione primaria è quella attiva, dunque la partizione Linux con la copia stage1. Eventualmente controllatelo con il comando `p` (print) di fdisk.

LILO

LILO può essere reinstallato da una copia di sicurezza dopo il ripristino di un MBR Windows. Verificate che il file di backup abbia la dimensione prescritta di 512 byte e ripristinatela con i seguenti comandi:

- Se LILO si trova nella partizione yyyy (per esempio hda1, hda2,...):

  ```
  dd if=/dev/yyyy of=nuovo-file bs=512 count=1
  dd if=file backup of=/dev/yyyy
  ```

- Se LILO si trova nell'MBR del disco zzz (per esempio hda, sda):

  ```
  dd if=/dev/zzz of=nuovo-file bs=512 count=1
  dd if=file backup of=/dev/zzz bs=446 count=1
  ```

L'ultimo comando è "cauto" e non scrive nella tabella di partizione. Anche qui *non dimenticate* di contrassegnare con fdisk come *attiva* (ingl. *bootable*) la partizione di avvio desiderata.

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, se disponete di un masterizzatore potete creare un CD di avvio su cui masterizzare i file di avvio di Linux.

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 (a partire da SuSE Linux 7.2):
  - ▷ Fate il boot dal CD/DVD di installazione come nel caso di una normale installazione.
  - ▷ Al boot selezionate l'opzione 'Installazione'. (Già di selezionata di default.)
  - ▷ Scegliete la lingua e la mappatura della tastiera.
  - ▷ 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 dati necessari per il boot di un sistema Linux (il bootloader Isolinux, il kernel ed initrd).

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

- Con il vostro editor preferito generate ora il file di configurazione del bootloader `/tmp/CDroot/isolinux.cfg`. Se usate per esempio `pico` il comando è

  ```
  pico /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 essere usate 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 KonCD che vi offre una superficie grafica opuure immettendo nella riga di comando:

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

  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 di `cdrecord` (`man cdrecord`)).

- Adesso provate il vostro CD di avvio! Riavviate il computer e verificate se il vostro sistema Linux si avvia correttamente dal CD.

Il sistema X-window

Sotto Unix il sistema X-window rappresenta quasi lo standard in tema di GUI (interfaccia grafica dell'utente), e questo non è tutto: X Window System detto anche X11, è un sistema basato sulla rete; l'output di applicazioni che girano sul computer `terra`, possono essere visualizzate su `sole`, sempre che i computer siano connessi via rete. La rete può essere una rete LAN, oppure WAN, cioè i computer possono anche essere distanti migliaia di chilometri e comunicare via Internet.

In questo capitolo, vi presenteremo tra l'altro xf86config che è un alternativa a SaX2 quando si tratta di configurare la scheda grafica, la tastiera ed il mouse. Parleremo inoltre della configurazione di OpenGL/3D. Per la descrizione dei moduli di YaST vedi [SuS03].

Un pò di storia

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. (dal 1996 ribattezzato The Open Group) ha portato avanti lo sviluppo dell'X Window System.

XFree86™ è un'implementazione libera dell' X-server per sistemi PC Unix (vedi `http://www.XFree86.org`); XFree86 è stato sviluppato e continua ad esserlo da programmatori sparsi in tutto il mondo, che nel 1992 si riunirono nel team XFree86. Da questo gruppo nacque la The XFree86 Project, Inc., fondata nel 1994, il cui scopo è mettere a disposizione l'XFree86™ ad un vasto pubblico e di collaborare all'ulteriore studio e sviluppo dell'X Window System; dal marzo del 2000 è disponibile per il download la major release XFree86 4.0 dal sito `http://www.XFree86.org`. Come standard, SuSE Linux esce con XFree86 86 4.x. Seguono informazioni dettagliate sulle proprietà della nuova versione.

Di seguito verrà trattata la configurazione dell' X-server. Si parlerà del programma xf86config con cui potrete configurare l'X Window System invece di ricorrere a SaX2 .

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

Attenzione

La configurazione del sistema X Window deve venire eseguita con estrema accuratezza. X non deve venire inizializzato prima che ne 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. Non si può comunque garantire in modo assoluto la correttezza dei metodi qui presentati ed escludere che possa venire danneggiato il vostro hardware.

Attenzione

La versione 4.x di XFree

Questa versione di SuSE Linux contiene l'attuale versione 4.x di XFree86, che si differenzia in alcuni punti dalla versione 3.3 finora contenuta nelle distribuzioni precedenti. Nell'uso della superficie grafica per l'utente questo si traduce in solo poche differenze, anche le applicazioni come per esempio il desktop grafico di KDE o GNOME continuano a comportarsi come nella versione 3.3.6.

Quali vantaggi offre la nuova versione?

Il nuovo X-server non è più un programma monolitico, bensì solo una struttura di base relativamente piccola a cui possono essere aggiunti dei moduli di programma necessari caricandoli all'occorrenza. Non ci sono quindi più (come nelle versioni precedenti) X-server supplementari per le diverse schede grafiche; vi è invece solamente un programma eseguibile chiamato XFree86 che troverete nella directory `/usr/X11R6/bin`. Questo è anche l'X-server vero e proprio. Il driver grafico che amministra l'indirizzamento della scheda grafica è un modulo caricabile.

Si procede in modo simile anche per quanto riguarda il supporto di diversi dispositivi di immissione (input device), font o protocolli X: anche qui vi sono dei singoli moduli che possono venire caricati in seguito dall'X-server. Generalmente non dovrete preoccuparvi più di tanto riguardo a questi moduli; la configurazione dei moduli necessari al funzionamento della superficie grafica del vostro computer, viene svolta quasi completamente da SaX2.

Grazie al concetto dei moduli, per il produttore diventa molto semplice implementare un driver per hardware speciale come per esempio schermi tattili o nuovissime schede grafiche. Gli sviluppatori hanno persino provveduto affinchè i moduli necessari per i diversi sistemi operativi possano venire messi a disposizione una sola volta; ciò significa che un modulo del driver grafico compilato per esempio sotto FreeBSD, può anche venire usato sotto Linux e viceversa. Questa portabilità è però limitata ad una sola piattaforma hardware; un modulo compilato per Linux su PowerPCs non può venire utilizzato su un PC Intel.

Inoltre il supporto del mouse è stato migliorato notevolmente. Soprattutto "sotto pressione", la reazione del mouse ai spostamenti è molto più veloce ed immediata rispetto al precedente X-server XFree86. Complessivamente è migliorata la velocità dell'output, in genere le operazioni grafiche vengono eseguite più velocemente che con il vecchio X-server (fatto dovuto alla rielaborata XAA (ingl. *XFree86 Acceleration Architecture*).

Rispetto a XFree86 3.3.x, il file di configurazione ha un formato un po' diverso. Se volete eseguire un "fine tuning" (una messa a punto finalizzata) del

vostro X-server, o se volete effettuare configurazioni speciali, troverete informazioni dettagliate nella sezione 5 a pagina 109 che si riferiscono alla struttura e al funzionamento del file di configurazione XFree86 che si trova adessi sotto `/etc/X11/XF86Config`. Anche il logging degli errori è migliorato: l'X-server crea un file di log molto dettagliato che troverete dopo l'avvio sempre nel file `/var/log/XFree86.0.log`.

Fra le caratteristiche della nuova versione vi è anche il supporto di opzioni speciali come per esempio True-Type-Font, la messa a disposizione dell'estensione di protocollo 3D glx, le correzioni gamma dello schermo e il supporto di più schede grafiche per configurazioni multihead. Sull'argomento vedi anche la sezione 5 a pagina 109.

Cosa cambia?

XFree86 4.0 si basa naturalmente sulla versione 3.3.x. Purtroppo, non si sono potuti portare tutti i driver grafici, poichè alcuni di essi sono molto complessi e non è stato possibile eseguire il porting sulla nuova architettura XAA.

Si tratta qui di schede grafiche utilizzate fin'ora con i seguenti X-server: XF86_S3, XF86_Mach8, XF86_Mach32 e XF86_8514. Ciò significa che tutte le schede S3 che necessitavano il server S3, non vengono supportate da XFree86 4.x: le schede S3 supportate fin'ora da server SVGA funzionano anche con XFree86 4.x. Nella maggior parte dei casi, si tratta di schede grafiche con chip S3 Trio3D, Savage4, Savage3D e Savage2000 e di quasi tutte le schede S3 Virge.

Le schede grafiche che per il funzionamento hanno bisogno degli X-server sopra citati (Mach8, Mach32 e 8514) non dovrebbero essere più tante.

Configurazione con xf86config

Per la semplice configurazione dell'X Window System, nella maggior parte dei casi SaX, come tool di configurazione, è superiore al programma xf86config. In alcuni rari casi una configurazione con SaX può fallire; allora potrete usare xf86config che in genere funziona sempre.

XFree86 4.x porta con sé un simile programma xf86config basato su testo; questo programma ha in alcuni punti dialoghi un po' modificati e scrive il file di configurazione naturalmente sotto `/etc/X11/XF86Config`. Nella seguente descrizione parleremo perciò solo del programma xf86config di XFree86 3.3.x.

Sotto XFree86 4.x, non è quasi mai richiesto l'uso di xf86config, poiché qui possono venire configurate anche le schede grafiche "problematiche" con il "frame buffer" o il modulo vga.

Per la configurazione servono i seguenti dati:

- Tipo di mouse, porta a cui è collegato il mouse e il baud rate con il quale il mouse viene usato (normalmente il baud rate è opzionale).
- Specifiche della scheda grafica.
- Dati del monitor (frequenze, etc.).

Se questi dati sono conosciuti o se avete a portata di mano la descrizione del monitor e della scheda, potete iniziare con la configurazione che può essere eseguita solo dall'utente `root`!

La configurazione viene inizializzata con:

```
terra:/root # xf86config
```

Mouse

Dopo la schermata di benvenuto, viene richiesto il tipo di mouse. Avrete la seguente lista per fare le vostre selezioni:

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

output 4: *Scelta del mouse per X*

Nello stabilire il tipo di mouse è da osservare che molti dei nuovi mouse Logitech sono compatibili con Microsoft oppure usano il protocollo MouseMan. La scelta Bus Mouse indica tutti i tipi di bus mouse, inclusi i Logitech!

Il tipo di mouse adatto viene scelto indicando il numero che lo precede. Eventualmente (p.e. alla scelta del tipo 1) segue la domanda se il ChordMiddle debba venire attivato: ciò è necessario con alcuni tipi di mouse o trackball per attivarne il tasto centrale:

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

Se si usa il mouse con due tasti, si può emulare il terzo tasto rispondendo alla prossima domanda con 'y':

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

Il terzo tasto del mouse viene emulato premendo contemporaneamente i due tasti del mouse.

La prossima domanda riguarda la porta a cui è collegato il mouse:

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

Se all'installazione del sistema è già stata indicata una porta per il mouse, confermate qui l'indicazione.

Tastiera

Ora vi si chiede se al tasto (Alt) sulla sinistra si debba essere correlato il valore Meta (ESC) e a quello destro il valore ModeShift (AltGr):

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

Rispondete qui con 'y' per poter inserire i caratteri della tastiera italiana indirizzabile tramite (Alt Gr) e affinché il tasto sinistro (Alt) possa venire usato come tasto meta – particolarmente vantaggioso quando si lavora con Emacs.

Monitor

Qui dovete specificare il monitor: la parte critica sono le frequenze verticali ed orizzontali che comunque vengono generalmente indicate nel manuale del monitor stesso.

Attenzione

Selezionare un intervallo di frequenza errato può danneggiare in modo irreparabile il vostro monitor! Il sistema X-Window indirizza solo modi video che gestiscono il monitor negli intervalli di frequenza indicati. L'indicazione di frequenze per le quali il monitor non è specificato, possono sovraccaricarlo!

Attenzione

Per alcuni monitor si possono consultare i valori sotto `/usr/X11R6/lib/X11/doc/Monitors` (comunque senza garanzia).

Per indicare la frequenza orizzontale viene presentata la seguente scelta:

```
hsync in kHz; monitor type with characteristic modes
 1 31.5;                Standard VGA, 640x480 @ 60 Hz
 2 31.5 - 35.1;         Super VGA, 800x600 @ 56 Hz
 3 31.5, 35.5;          8514 Compatible, 1024x768 @ 87 Hz interl.
                        (no 800x600)
 4 31.5, 35.15, 35.5;   Super VGA, 1024x768 @ 87 Hz il.,
                        800x600 @ 56 Hz
 5 31.5 - 37.9;         Extended Super VGA, 800x600 @ 60 Hz,
                        640x480 @ 72 Hz
 6 31.5 - 48.5;         Non-Interlaced SVGA, 1024x768 @ 60 Hz,
                        800x600 @ 72 Hz
 7 31.5 - 57.0;         High Frequency SVGA, 1024x768 @ 70 Hz
 8 31.5 - 64.3;         Monitor that can do 1280x1024 @ 60 Hz
 9 31.5 - 79.0;         Monitor that can do 1280x1024 @ 74 Hz
10 Enter your own horizontal sync range
Enter your choice (1-10):
```

output 5: *Indicare le frequenze orizzontali del monitor*

Usate una di queste indicazioni, solo se non conoscete i dati esatti del monitor. Scegliendo il punto '10' potete specificare le frequenze esatte.

Dopo l'indicazione delle frequenze orizzontali, vengono richieste quelle verticali. Anche qui potete scegliere:

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

 Enter your choice (1-5):
```

output 6: *Frequenze verticali dettagliate*

Anche in questo caso è preferibile indicare frequenze precise, piuttosto che scegliere uno dei punti da '1' a '4'.

Viene quindi richiesta l'indicazione di un nome per la descrizione del monitor,

```
Enter an identifier for your monitor definition:
```

l'indicazione del produttore,

```
Enter the vendor name of your monitor:
```

e l'indicazione del modello

```
Enter the model name of your monitor:
```

Qui potete indicare il nome relativo o, con (Enter), accettare i valori predefiniti: con ciò si termina l'impostazione del monitor.

Scheda grafica/X-server

Passiamo ora a specificare la scheda grafica utilizzata:

```
Do you want to look at the card database?
```

Rispondendo con 'y' viene presentata una lista di schede grafiche preconfigurate.

Da questa lista, indicando il numero relativo, si può scegliere una definizione di scheda: non si dovrebbe però accettare una definizione qualsiasi, poiché anche nelle schede dello stesso tipo possono esserci differenze per quanto riguarda il clock-chip e RAMDAC (ingl. **R***andom* **A***ccess* **M***emory* **D***igital-to-***A***nalogue* **C***onverter*)!

Per questa ragione, nonostante sia stata scelta una definizione, più avanti verrano comunque chiesti nuovamente clock-chip, Ramdac, ecc. Vi sarà comunque un'ulteriore opzione derivante dal valore predefinito della definizione di scheda.

Le definizioni delle schede contengono informazioni sul clock-chip, Ramdac e sull'X server da utilizzare. Nella device section del file `XF86Config`, vengono riportate preziose indicazioni sull'uso della scheda.

Non preoccupatevi se la vostra scheda non è inclusa nell' elenco: in questo caso con 'q' si può ritornare alla normale configurazione. Tenete presente che potete selezionare una scheda grafica solo se coincide esattamente con la scheda che utilizzate! La scelta di una scheda con una nome simile non è consigliabile: nomi simili non sono garanzia di hardware simile...

Altre informazioni sulla configurazione della scheda grafica, vengono riportate nel capitolo 5 a pagina 109.

Dopo aver specificato la scheda segue la scelta dell'X server:

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

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

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

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

output 7: *Scelta del X-server*

1 Un server per monitor monocromatici (bianco/nero). Dovrebbe funzionare con ogni scheda grafica VGA o compatibile e offrire almeno una risoluzione di 640x480 pixel.

2 Il server XF86_VGA16 a 16 colori. Dovrebbe funzionare con ogni scheda grafica VGA o compatibile.

3 Il server SVGA XF86_SVGA. Questo server a 256 colori supporta una grande quantità di schede SVGA. Con alcune schede Cirrus e WD viene sfruttata l'accelerazione hardware della scheda. Con alcune schede Cirrus può anche venire attivata la modo colori a 16 o 32 bit.

4 Server per schede grafiche accelerate: qui si possono scegliere più server (vedi sotto).

5 Questo punto è interessante solo se nella scelta precedente avete selezionato una definizione della scheda. Qui viene proposto il server adatto alla scheda selezionata.

Una volta scelto il server, viene chiesto se si debba creare un link simbolico dal server scelto a `/usr/X11R6/bin/X`. Se la risposta è affermativa,'y', seguirà la domanda se il link debba venir creato in `/var/X11R6/bin`:

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

Rispondete affermativamente a questa domanda, poiché può darsi che non si possa scrivere su `/usr`. Se alla selezione sopra indicata avete scelto '4', appare un menu con gli X server disponibili per le schede grafiche accelerate:

```
Select an accel server:

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

Which accel server:
```

Questi server supportano la scheda corrispondente. Generare dei link presuppone che il server adatto sia già stato installato, cioè, che al momento della installazione dell' X Window System è stato già selezionato il server giusto. Dopo la scelta dell'X-server, si deve specificare la scheda grafica. Per prima cosa si richiedono informazioni sulla memoria video della scheda grafica:

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

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

Enter your choice:
```

output 8: *Indicazione della memoria grafica*

Alla fine viene richiesto il nome, il produttore e il tipo della scheda. Se è stata scelta una scheda grafica, è sufficiente premere ↵.

```
Enter an identifier for your video card definition:

Enter the vendor name of your video card:

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

Se come X server avete scelto un server per schede grafiche accelerate, vi vengono richieste le impostazioni RAMDAC; queste impostazioni sono rilevanti solo per i server S3 e AGX:

```
 1  AT&T 20C490 (S3 server)                        att20c490
 2  AT&T 20C498/21C498/22C498 (S3)                 att20c498
 3  AT&T 20C505 (S3)                               att20c505
 4  BrookTree BT481 (AGX)                          bt481
 5  BrookTree BT482 (AGX)                          bt482
 6  BrookTree BT485/9485 (S3)                      bt485
 7  Sierra SC15025 (S3, AGX)                       sc15025
 8  S3 GenDAC (86C708) (autodetected)              s3gendac
 9  S3 SDAC (86C716) (autodetected)                s3_sdac
10  STG-1700 (S3)                                  stg1700
11  TI 3020 (S3)                                   ti3020
12  TI 3025 (S3)                                   ti3025
13  TI 3020 (S3, autodetected)                     ti3020
14  TI 3025 (S3, autodetected)                     ti3025
15  TI 3026 (S3, autodetected)                     ti3026
16  IBM RGB 514 (S3, autodetected)                 ibm_rgb514
```

```
 17  IBM RGB 524 (S3, autodetected)                  ibm_rgb524
 18  IBM RGB 525 (S3, autodetected)                  ibm_rgb525
 19  IBM RGB 526 (S3)                                ibm_rgb526
 20  IBM RGB 528 (S3, autodetected)                  ibm_rgb528
 21  ICS5342 (S3, ARK)                               ics5342
 22  ICS5341 (W32)                                   ics5341
 23  IC Works w30C516 ZoomDac (ARK)                  zoomdac
 24  Normal DAC                                      normal
```

output 9: *Indicazioni del RAMDAC*

Nella maggioranza dei casi la cosa migliore è quella di premere Invio senza effettuare nessuna scelta. Una volta selezionata una scheda grafica che appoggi una determinata impostazione RAMDAC, ciò viene indicato e dovrebbe venire selezionato.

Dopo aver risposto a queste domande, si può scegliere il clock chip (sempre che sia presente), per le schede accelerate. Grazie alla scelta di un clock chip, non sono più necessarie le righe clock, poiché i clock necessari possono venire programmati:

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

output 10: *Indicazione del clock chip*

Se avete una scheda grafica sprovvista di clock chip, basta premere Invio per non dover selezionare alcun clock chip. Se avete scelto una scheda grafica dal menu di selezione, il clock chip, se esiste, viene indicato automaticamente.

Se non è stato scelto alcun clock chip, xf86config propone di inizializzare X -probeonly per determinare i clock-timing supportati dalla scheda che vengono registrati automaticamente in una riga Clocks del file `XF86Config`.

A questo punto dobbiamo dire perché i clock timing rilevati e registrati automaticamente siano **tanto pericolosi**: se la scheda grafica ha un clock chip programmabile, l'X server non è in grado di passare da un clock all'altro della scheda e riconosce perciò solo i clock 0, 1 e a volte il 2. Tutti gli altri valori sono più

o meno casuali (in generale i clock 0, 1 e 2 si ripetono e vengono perciò sostituiti da zeri.)

Tutti i clock, tranne 0 e 1, dipendono in prima linea dalla preprogrammazione del clock chip: p.e., al momento del rilevamento il clock 2 potrebbe aver avuto un altro valore (che è stato registrato in `XF86Config`) rispetto a quello che verrà rilevato più tardi all'avvio dell'X-server. Tutti i timing non corrispondono più e il monitor potrebbe venire danneggiato.

Un buon segno di riconoscimento per un clock chip programmabile e dei problemi connessi, sono i molti zeri o i valori timing che si ripetono. Tali valori non devono assolutamente essere assunti nel file `XF86Config`!

Usate perciò la seguente strategia per determinare i clock chip o i clock timing:

- La cosa migliore è di indicare un **clock chip programmabile** esistente (sempre che ce ne sia uno): questi verrà quindi programmato in modo adeguato e l'`XF86Config` non conterrà indicazioni clock. Potete anche confrontare i chip della scheda con i clock chip offerti nel menu e, in questo modo, trovare il chip giusto. Quasi tutte le moderne schede S3 hanno un clock chip programmabile.

- Se sulla scheda grafica non vi è **alcun clock chip programmabile**, inizializzate `X -probeonly` e paragonate (a computer non sotto carico) i valori clock determinati con quelli del manuale della scheda grafica. Se i valori corrispondono approssimativamente (± 2), riportateli nel file `XF86Config`.

  Se non doveste trovare la risposta che cercate nel manuale, potete far determinare i valori di timing con `X -probeonly` (si consiglia a computer non sotto carico). Esaminate la validità dei valori determinati, poiché i valori clock di alcune schede sono illegibili (molti zeri o valori ripetuti indicano valori non validi). Riportate voi stessi i valori validi nel file `XF86Config`. Non tralasciate o dimenticate alcun valore, non cercate assolutamente di cambiar ordinei o di modificarli: essi devono venire registrati esattamente nella stessa sequenza.

  Se avete un server P9000, si deve semplicemente indicare nella riga Clock, per ogni modalitá e in una qualsiasi sequenza, il clock desiderato.

- In linea di massima vale: nei clock chip programmabili non deve esserci la riga Clocks nell'`XF86Config` (eccezione: P9000).

  Per schede senza clock chip programmabili, dovrebbe esistere una riga '*Clocks*' nell'`XF86Config`: tramite essa si può evitare il fastidioso ed a volte pericoloso rilevamento automatico dei clock ad ogni avvio del sistema X-Window. Inoltre con schede il cui clock non è leggibili non ci saranno valori errati e quindi nessun pericolo per il vostro monitor.

Se, dopo aver letto attentamente i paragrafi precedenti, desiderate provare a far rilevare automaticamente i clock, alla domanda:

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

rispondete affermativmente 'y'. Per un alcuni attimi lo schermo si annerirà e alla fine apparirà una lista dei clock rilevati o la comunicazione che non è stato rilevato alcun clock. Se è stato selezionato un clock-chip, non apparirà la domanda se debba venire inizializzato X -probeonly poiché i clock vengono impostati automaticamente. In questo caso si passa direttamente al prossimo punto di configurazione.

Attenzione

Se avete risposto affermativamente all'ultima domanda e lo schermo si annera per più di 30 secondi, interrompete il test con Ctrl +Alt +← o Ctrl +c! Se necessario, devono venire spenti il computer e il monitor per non correre il rischio di danneggiare l'hardware!

Attenzione

Memorizzare la configurazione

A questo punto la configurazione è conclusa; vi resta di memorizzare il file di configurazione. È consigliabile memorizzare il file di configurazione X-Window `XF86Config` nella directory `/etc`. In questo modo, si garantisce che anche nella rete, ogni computer abbia una "propria" configurazione, anche se più computer condividono il file system `/usr`.

A questo punto salvate `/etc/XF86Config`! – E così terminate il programma xf86config e il processo di configurazione dell'X Window System.

Come ottimizzare l'installazione del sistema X Window

In questo capitolo descriveremo la struttura del file di configurazione `/etc/X11/XF86Config`. Questo file è suddiviso in sezioni introdotte dalla parola chiave Section "identificatore", e terminano con EndSection. Ci limiteremo a presentare le sezioni principali.

In seguito indicheremo come integrare ulteriori font, come configurare gli input device e come abilitare l'acceleramento 3D. Questo viene naturalmente eseguito

anche in determinate sezioni del file `XF86Config`, ma l'integrazione di ulteriori font richiede il ricorso a programmi esterni che però vengono forniti con SuSE Linux o fanno parte dell'installazione di default. I procedimenti qui accennati intendono solo presentare le possibilità esistenti e servire da stimolo, e non hanno certamente la pretesa di essere completi.

I programmi SaX2 e xf86config (per XFree86 4.x) 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 indicazioni su 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:

Tipo	Significato
Files	Questa sezione descrive i path 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'ingresso. Contrariamente a XFree86 3.3, vengono configurati tramite questa sezione sia tastiere che mouse che speciali dispositivi di ingresso 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.

Tabella 5.1: *Continua alla pagina seguente...*

Modes	Qui vengono definiti i parametri di rappresentazione delle singole risoluzioni dello schermo. Questi parametri possono venire calcolati da SaX2 in base a 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; troverete una definizione dettagliata dei singoli valori numerici nel file HOWTO andando su `/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 congiunge un `Monitor` e un `Device` e ne derivano le indicazioni necessarie per XFree86. La sottosezione `display` permette l'indicazione della 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'ingresso `InputDevice` e quelli di uscita `Screen`.

Tabella 5.1: *Sezioni in /etc/X11/XF86Config*

Occupiamoci ora delle sezioni `Monitor`, `Device` e `Screen`. Nella pagina di manuale di `XF86Config` (`man 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`.

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.

Una sezione screen può assumere p.e. l'aspetto di 3.

```
Section "Screen"
  DefaultDepth  16
```

```
  SubSection "Display"
    Depth       16
    Modes       "1152x864" "1024x768" "800x600"
    Virtual     1152x864
  EndSubSection
  SubSection "Display"
    Depth       24
    Modes       "1280x1024"
  EndSubSection
  SubSection "Display"
    Depth       32
    Modes       "640x480"
  EndSubSection
  SubSection "Display"
    Depth       8
    Modes       "1280x1024"
  EndSubSection
  Device        "Device[0]"
  Identifier    "Screen[0]"
  Monitor       "Monitor[0]"
EndSection
```

file 3: *La sezione Screen del file /etc/X11/XF86Config*

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, già definiti prima nel file. Si tratta in fondo di rimandi alle sezioni device e monitor con i rispettivi nomi. Entreremo nei dettagli riguardanti queste sezioni più avanti.

Tramite l'indicazione `DefaultColorDepth`, 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, 24 e 32. Non tutti i moduli dell'X server supportano ognuno di questi valori; 24 e 32 bpp hanno la stessa profondità di colori, con la differenza che 24 sceglie il modo 24 bpp packed-pixel e 32 il modo 24 bpp padded-pixel.

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 mode, 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 `Depth16` 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 8 bit - può avere fino a 4096x4096(!) pixel. Specialmente con server accelerati non è consigliabile usare per lo schermo virtuale l'intera memoria della scheda grafica, poiché la memoria inutilizzata viene dedicata da questi server a diverse font cache ed alla cache grafica.

Device-Section

Una device section descrive e definisce una determinata scheda grafica. `XF86Config` può contenere diverse device section, sempre che abbiano un nome diverso, il quale viene indicato dalla parola chiave Identifier. 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 rilevati 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. I driver vengono cercati dall'X-server nella sottodirectory `driver` per via di ModulePath definito nella sezione Files. Nel caso della Matrox Millennium, il modulo driver si chiama mga. 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 generalmente valide si trovano nella pagina di manuale di `XF86Config` (`man XF86Config`) e nella pagina di manuale di `XFree86` (`man XFree86`).

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 (ed in particolar modo 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 [FCR93], in cui vengono dettagliatamente 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.

Inserire ulteriori font (TrueType)

Una buon numero di font fa parte di una normale installazione X-server X11R6 che troverete nella directory `/usr/X11R6/lib/X11/fonts` raggruppati in sottodirectory. Ricordate che l'X-server considera solo sottodirectory:

- che sono registrate come `FontPath` nella sezione Files del file `/etc/X11/XF86Config`
- che possiedono un file `fonts.dir` valido
- che non sono state disabilitate durante il funzionamento dell'X-server con il comando xset −fp
- o che sono state abilitate durante il funzionamento dell'X-Server con il comando xset +fp

Dalla versione 4.0, XFree86 non supporta soltanto il proprio formato Type1 (un formato PostScript) per font set scalabili e pcf per bitmap font set, ma anche il formato ttf (ingl. *true type font*). Come già visto nella sezione 5 a pagina 99, questo supporto viene naturalmente realizzato tramite moduli caricabili dell'X-server. Potete quindi usare con l'X-server anche directory che contengono font True-Type senza preparativi preliminari.

Un grande vantaggio di quasi tutti i font true-type (oltre alla buona scalabilità), consiste nel fatto che questi font contengono praticamente sempre molto di più dei normali 255 caratteri del font set codificato in "iso-8859-1" per l'Europa occidentale. Con questi font set avrete a vostra disposizione lettere cirilliche, greche o dell'Europa orientale, e con software speciale anche quelle di lingue asiatiche. Qui vogliamo descrivere, come esempio, l'uso di font a 8 Bit. Se volete inserire caratteri di lingue asiatiche, (giapponese, cinese etc.), potete usare editor speciali disponibili anche sotto SuSE Linux.

Un font a 8 bit comprende 255 caratteri e completa l'ASCII-font americano in cui sono definiti solo i primi 128 dei 255 possibili caratteri. Un carattere occupa quindi 8 bit nella memoria del computer. Poiché 127 caratteri non sono assolutamente sufficienti per rappresentare tutti i caratteri speciali delle lingue europee, le diverse lingue vengono raggrupate e ogni gruppo ottiene un nome breve. Il relativo font set viene indicato secondo la relativa norma come font set "iso-8859-x", in cui x è una cifra tra 1 e 15. L'esatta successione dei caratteri nel font set iso-8859-1 o iso-8859-15, potete desumerla dalla pagina di manuale di `iso-8859-1` (`man iso-8859-1`) e rispettivamente dalla pagina di manuale di `iso-8859-15` (`man iso-8859-15`).

Le codificazioni più conosciute si trovano nella tabella 5.2, altre codificazioni potete desumerle dalla suddetta pagina di manuale.

Font set	**Regioni supportate, contiene caratteri speciali**
iso-8859-1	Lingue dell'Europa occidentale: spagnolo, tedesco, svedese, danese, ecc.; per il finlandese ed il francese è ormai preferibile utilizzare `iso-8859-15`
iso-8859-2	Europa centro-orientale: ungherese, ceco, rumeno, polacco, tedesco, ecc.
iso-8859-5	Caratteri cirillici per il russo
iso-8859-7	Caratteri greci per il greco
iso-8859-9	Caratteri per il turco
iso-8859-15	Simile a iso-8859-1, ma con il simbolo dell'Euro e miglior supporto per il finlandese e francese.

Tabella 5.2: *I codici principali*

L'utente deve scegliere la codificazione adatta in base alla lingua selezionata. Specialmente scambiandosi testi tra diversi computer deve venire trasmessa anche la codificazione utilizzata. Il vantaggio del procedimento consiste nel fatto che per avere il supporto dei caratteri speciali regionali, basta scegliere la codificazione giusta e subito (quasi) tutti i programmi potranno raffigurare questi caratteri speciali, poiché quasi tutti i programmi usano un valore di 8 bit (un byte) per la rappresentazione di un carattere di testo. Se si seleziona la codificazione sbagliata, anche i caratteri speciali vengono raffigurati in modo errato. Nella maggioranza delle applicazioni X, e anche nel desktop di KDE, potete scegliere la codificazione del font set, quasi sempre con la configurazione del font set da usare. Nelle applicazioni X, di solito la codificazione viene quasi sempre indicata con il nome `encoding`.

Lo svantaggio di questo approccio è che alcune combinazioni sono semplicemente impossibili: non è per esempio per nulla semplice redigere un testo tedesco con metafonia inserendovi nomi di paesi russi in cirillico.

Questo dilemma può venire risolto ricorrendo a Unicode. Unicode non codifica caratteri – diversamente da ASCII – con un byte, bensì con 2 o più byte cosicchè possono venire raffigurati molti più caratteri. Con l'uso di Unicode potete raffigurare anche le lingue asiatiche con più di 127 caratteri, come il cinese o giapponese o coreano. Lo svantaggio di questa soluzione, è che la maggior parte del software esistente, non è preparato all'uso di questi caratteri ed è possibile leggere o scrivere testi con caratteri Unicode solo con software speciale. Altre informazioni sull'uso di font unicode sotto Linux, si trovano sotto `http://www.unicode.org`. Per il futuro ci si attende comunque che sempre più programmi supporteranno caratteri Unicode. SuSE Linux vi offre il programmayudit con il quale potete editare testi in Unicode. Il pacchetto si trova nel pacchetto `yudit`, serie `xap` o, dopo l'installazione, nel menu di SuSE sotto Professionale/Office e lì sotto Editor.

Ed ecco ora passo per passo, la descrizione dell'installazione dei font set supplementari sull'esempio dei font true type.

Trovate i font che volete installare nel vostro X Window System. Se sul vostro sistema avete font true type vincolati da licenza, potete usarli. Montate la partizione che contiene questi font ed entrate nella directory dei font.

SuSE Linux ha già preparato una directory con il nome `/usr/X11R6/lib/X11/fonts/truetype`; potete copiarci i font in questione.

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

Create dei link sui file `ttf`. Immettete il percorso corretto al posto di ⟨*/path/del/font*⟩ sotto cui il font deve essere disponibile. Lanciate SuSEconfig che creerà le registrazioni necessarie nel file `fonts.dir`.

```
terra:/usr/X11R6/lib/X11/fonts/truetype #
     ln -s ⟨/path/del/font⟩/*.ttf .
terra:/usr/X11R6/lib/X11/fonts/truetype #
     SuSEconfig -module fonts
```

Se l' X-Server è in esecuzione, potete rendere disponibili i font in modo dinamico. Digitate:

```
terra:~ #  xset fp rehash
```

Suggerimento

Il comando `xset` accede all'X-server tramite il protocollo X, quindi deve disporre dei permessi di accesso all'X-server in esecuzione, ad esempio, nel caso in cui `tux` sia l'utente che ha inizializzato l'X-server. Per ulteriori informazioni, consultate la pagina di manuale di `xauth` (`man xauth`).

Suggerimento

Controllate che i font siano stati configurati in modo corretto; per farlo usate il comando xlsfonts. Se i set dei caratteri sono installati correttamente, si ottiene l'elenco di tutti i font installati, incluso i nuovi font true type. Potete anche usare il fontmanager di KDE, che vi fornisce degli esempi di testo con i font installati che potete lanciare tramite il centro di controllo di KDE.

```
terra:~ #  xlsfonts
```

I font integrati in questo modo possono venire usati da tutte le applicazioni di X.

Configurare OpenGL/3D

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

Supporto hardware

SuSE Linux contiene molti driver OpenGL per il supporto hardware 3D. Ecco una rassegna nella tabella 5.3.

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

Tabella 5.3: *Hardware 3D supportato*

Se effettuate una nuova 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, il driver "dummy" incluso dovrà essere sostituito dal driver ufficiale di nVidia. Scaricatelo dal server web di nVidia (`http://www.nvidia.com`) ed installatelo. Per motivi di licenza, possiamo fornire solo un driver nVidia "dummy".

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.

Driver OpenGL

nVidia-GLX e DRI

Questo driver OpenGL può essere configurato abbastanza comodamente usando SaX2. Se avete una scheda nVidia dovete sostituire il driver nVidia "dummy" attraverso un driver da scaricare dal sito web di nVidia (`http://www.nvidia.com`). Con il comando `3Ddiag`, controllate che nVidia-GLX e DRI siano configurati correttamente.

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 (nVidia-GLX) 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.

Tool di diagnosi 3Ddiag

Per verificare 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 di supporto 3D sono 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 ammessi per 3Ddiag.

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".

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 4.x. 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, rimane il Software Rendering Fallback del driver DRI, che 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.

Supporto all'installazione

A parte il Software Rendering Fallback del driver DRI i driver OpenGL sotto Linux si trovano in fase di sviluppo e devono pertanto essere considerati 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.

Ulteriore documentazione in linea

- DRI: `/usr/X11R6/lib/X11/doc/README.DRI` (il pacchetto `XFree86-doc`)
- Mesa in generale: `/usr/share/doc/packages/mesa/` (il pacchetto `mesa`)

Stampare

Questo capitolo riassume i principi fondamentali della stampa in Linux. Gli esempi consentiranno di comprendere i nessi del processo di stampa che a sua volta permetterà di riconoscere e risolvere più celermente degli eventuali problemi.

Principi

Con Linux le stampanti vengono indirizzati attraverso cosiddette code di stampa (print queue).

I dati da stampare vengono memorizzati temporaneamente nella code 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 compreso dalla stampante. Il cosiddetto filtro della stampante si occupa della traduzione dei dati da stampare in un linguaggio compreso dalla stampante.

Esempi di linguaggi di stampante standard

Testo in ASCII La maggior parte delle stampanti è in grado di stampare direttamente almeno testi ASCII. Le stampanti che fanno eccezione, cioè che non stampano direttamente testi ASCII, vengono indirizzati da uno dei seguenti linguaggi di stampante standard.

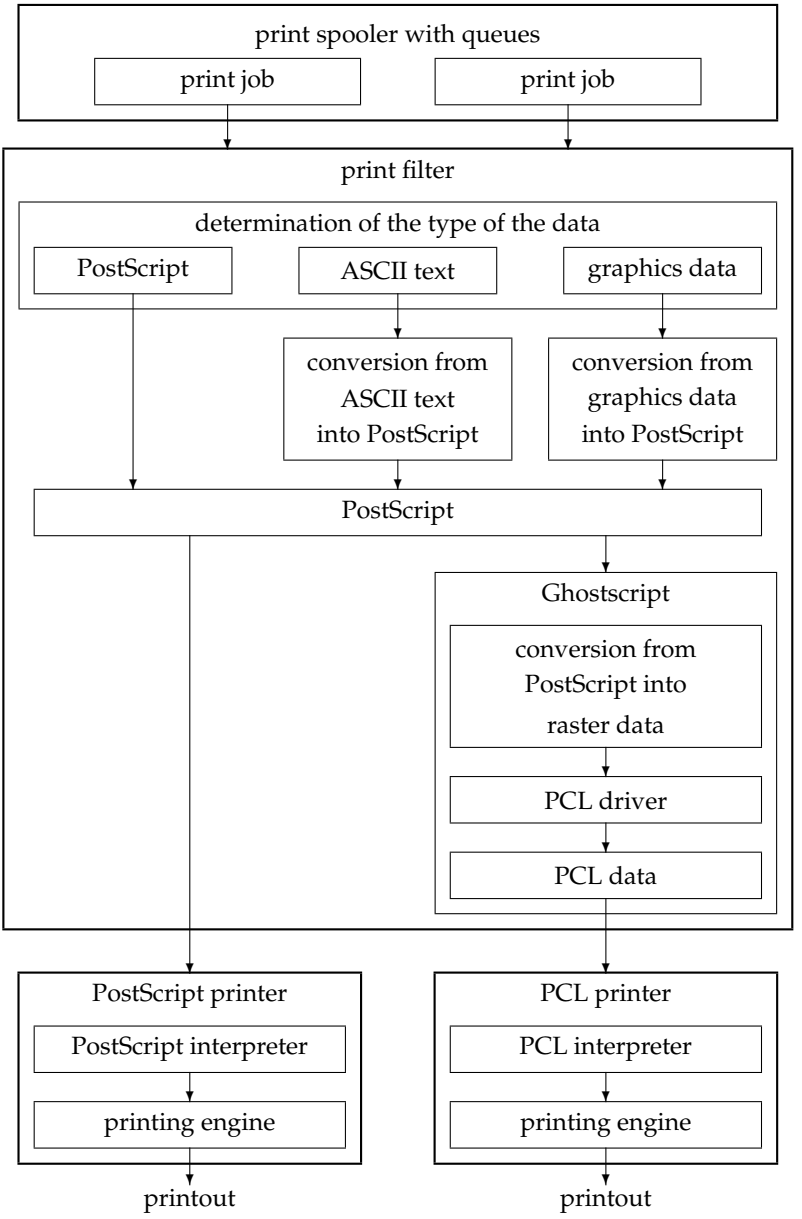
PostScript PostScript è il linguaggio standard di Unix/Linux, che permette di stampare direttamente con stampanti PostScript. Queste stampanti sono relativamente costose, visto che PostScript è un linguaggio potentissimo ma complesso che richiede dalle stampanti PostScript una laboriosa elaborazione 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 usa il programma Ghostscript per convertire i dati in uno di questi linguaggi di stampante standard. Viene utilizzato un driver Ghostscript confacente il più possibile al modello della stampante, in modo da considerare le particolarità del modello, per esempio le impostazioni del colore.

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) determinato 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 con il programma `a2ps`.
   (c) dati PostScript vengono convertiti eventualmente in un altro linguaggio di stampante.
      - Nel caso di stampanti PostScript, i dati PostScript vengono inviati direttamente alla stampante.
      - Altrimenti il programma Ghostscript viene utilizzato con un driver Ghostscript adatto al relativo modello di stampante per generare i dati da inviare infine alla stampante.
4. Dopo che l'incarico di stampa è stato inviato completamente alla stampante, lo spooler della stampante cancella l'incarico dalla coda.


print spooler with queues
print job
print job
print filter
determination of the type of the data
PostScript
ASCII text
graphics data
conversion from ASCII text into PostScript
conversion from graphics data into PostScript
PostScript
Ghostscript
conversion from PostScript into raster data
PCL driver
PCL data
PostScript printer
PostScript interpreter
printing engine
PCL printer
PCL interpreter
printing engine
printout
printout

Diversi sistemi di stampa

SuSE Linux supporta due tipi di 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 viene stabilita dall'amministratore di sistema, ed l'utente può solamente scegliere tra le diverse code. Al fine di poter scegliere tra diverse configurazioni per una stampante, si devono impostare diverse code con configurazioni diverse per la stessa stampante. Con le semplici stampanti monocromatiche (per esempio 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 e fotostampe. Attraverso le configurazioni stabilite da una parte viene assicurato che vengono utilizzate solo le configurazioni impostate dall'amministratore di sistema; dall'altra però viene preclusa ogni possibilità all'utente di eseguire qualunque impostazione personale. Per l'amministratore di sistema questo significa dover impostare di conseguenza tante code, se deve essere reso disponibile l'elevato numero di funzionalità delle stampanti moderni.

CUPS – Nel sistema di stampa CUPS l'utente ha la possibilità di stabilire impostazioni specifiche della stampante per ogni incarico di stampa. In questo sistema la configurazione della coda non viene stabilita per intero dall'amministratore di sistema, ma le possibilità di impostazioni specifiche della stampante sono deposte per ogni coda in un file sì detto PPD (ingl. *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 incompatibili, di solito non è possibile installare entrambi i sistemi di stampa *contemporaneamente*; YaST comunque permette di passare dall'uno all'altro sistema di stampa – vedi sezione *Configurare la stampante con YaST* a pagina 133.

Indicazioni generali per problemi con la stampante

Nella documentazione vengono descritte innanzitutto questioni generali e come risolverli. Per tanti problemi specifici trovate una soluzione nella banca dati di supporto (inglese).

Se avete dei problemi con la stampante gli articoli della banca dati di supporto *Installing a Printer* e *Printer Configuration with SuSE Linux 8.2* rappresentano il punto di partenza che trovate con la parola chiave "Printer" o online sotto:
`http://sdb.suse.de/en/sdb/html/jsmeix_print-einrichten.html`
`http://sdb.suse.de/en/sdb/html/jsmeix_print-einrichten-82.html`
Soprattutto l'ultimo articolo si riferisce alla "configurazione della stampante con SuSE Linux 8.2".

La banca dati di supporto si trova inoltre nel sistema di aiuto di SuSE o online sotto `http://sdb.suse.de/en` trovate la versione sempre aggiornata.

I problemi principali rilevati per ogni versione vengono riassunti in un articolo:
Problemi noti e particolarità in SuSE Linux 8.2
`http://sdb.suse.de/en/sdb/html/bugs82.html`
Problemi noti e particolarità in SuSE Linux 8.1
`http://sdb.suse.de/en/sdb/html/bugs81.html`
Se non doveste trovare la risposta che cercate né nella documentazione acclusa né nella banca dati di supporto, vi offriamo volentieri assistenza nel quadro del servizio di supporto di SuSE. Per avere ulteriori informazioni andate su `http://www.suse.de/it/services/support/index.html` o per l'utenza business:
`http://www.suse.de/en/business/services/support/index.html`

Premesse per stampare

Prerequisiti generali

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

  Banca dati delle stampanti di SuSE – `http://cdb.suse.de/en` oppure `http://hardwaredb.suse.de/en`.

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

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

SuSE Linux driver Ghostscript – `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 *Configurazione manuale delle porte di una stampante locale* a pagina 139 o la sezione *Configurazione manuale* a pagina 136.
- 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 originale SuSE ed eseguire il reboot con questo kernel.
- Vi raccomandiamo di installare il 'Sistema standard' con YaST, per assicurare che tutti i pacchetti necessari siano disponibili. E' bene che durante l'installazione del sistema standard non deselezionate dei pacchetti preselezionati, altrimenti installate almeno il 'Sistema standard'. I 'sistemi minimali' non bastono per stampare.

Determinare il driver adatto alla stampante

La stampante PostScript non necessita di speciali driver. Vedi a riguardo la sezione *Il processo di stampa* a pagina 124. Per stampanti non-PostScript è un driver Ghostscript a creare i dati da stampare. Per tale ragione è il driver Ghostscript a determinare il risultato prodotto delle 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 *Prerequisiti generali* nella pagina precedente indicano anche driver Ghostscript per singoli modelli di stampante.

Eventualmente chiedete al produttore della stampante, quale sia il linguaggio della vostra stampante o con quale modello della banca dati delle stampanti sia compatibile la vostra stampante (vedi sotto). Soprattutto con nuovi modelli è facile dire se la stampante è atta a funzionare sotto Linux. Anche qui le differenze in tema di supporto Linux dipendono dai vari produttori.

Se nemmeno il produttore dovesse essere in grado di fornire delle informazioni sulla vostra stampante riguardo alla compatibilità con Linux, seguite queste indicazioni:

- Verificate se la vostra stampante è compatibile con un modello che gira sotto Linux e utilizzate il driver Ghostscript del modello compatibile. Compatibile con Linux 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 per emularlo (per un altro sistema operativo). Simili denominazioni delle stampanti non significa necessariamente 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 in modo diretto dovrebbero funzionare con il driver Ghostscript ljet4 fino a 600x600 dpi. Spesso PCL5e viene indicato solo con PCL5.

  PCL4 o PCL5 – Stampanti che comprendono PCL4 o PCL5 dovrebbero funzionare con i driver Ghostscript laserjet, ljetplus, ljet2p o ljet3, comunque vi è una restrizione di 300x300 dpi.

  PCL3 Stampanti che comprendono 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 stcolor o uniprint assieme ad un file parametro adatto *.upp (per esempio stcany.upp).

Stampanti GDI

Dato che i driver per stampanti di solito non vengono sviluppati dal produttore dell'hardware per Linux, bisogna indirizzare la stampante attraverso un linguaggio generalmente compreso come PostScript, PCL ed 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 funzionante 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 conosciute, non è possibile, o solo accompagnato da tante difficoltà, utilizzare questi dispositivi fuori dalla norma con Linux.

GDI è una interfaccia di sviluppo concepita dalla Microsoft per la rappresentazione grafica. Il problema non è l'interfaccia di programmazione ma il 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 (per esempio una risoluzione minore).

Vi sono inoltre delle particolari stampanti che comprendono il linguaggio standard solo in parte - 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 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 esitono 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 dai produttori per questo tipo di stampanti a produrre i migliori risultati.

Le seguenti stampanti GDI sono supportate direttamente da SuSE Linux e potrete configurarle per mezzo di YaST; visto che comunque le stampanti GDI

causano spesso dei problemi, può accadere che alcuni modelli non funzionano o vi sono delle vistose restrizioni (per esempio 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 modelli compatibili.
- HP DeskJet 710/712/720/722/820/1000 e modelli compatibili.
- Lexmark 1000/1020/1100/2030/2050/2070/3200/5000/5700/7000/7200, Z11/42/43/51/52 e modelli compatibili. Driver Linux direttamente della Lexmark si trovano sotto `http://www.lexmark.com/printers/linuxprinters.html`
- Oki Okipage 4w/4w+/6w/8w/8wLite/8z/400w e modelli compatibili.
- Samsung ML-200/210/1000/1010/1020/1200/1210/1220/4500/5080/6040 e modelli compatibili.

Le seguenti stampanti GDI – almeno per quanto ne sappiamo – non sono supportate da SuSE Linux; comunque l'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

Configurare la stampante con YaST

Code di stampa e configurazione

Solitamente sono necessarie più code per i seguenti motivi:

- Diverse stampanti differenti devono essere indirizzate attraverso code diverse.
- Il filtro della stampante può essere configurato individualmente per ogni coda; questo significa che vengono utilizzate differenti code per la stessa stampante per mettere a disposizione differenti configurazioni. Questo non è necessario con CUPS, poiché qui l'utente può eseguire delle impostazioni proprie; si veda a riguardo la sezione *Diversi sistemi di stampa* a pagina 127

Con stampanti in bianco e nero (per esempio la maggioranza delle stampanti laser) basta una configurazione standard, ma per stampanti a getto di inchiostro a colore servono almeno due tipi di configurazione — dunque due code:

- Una configurazione "lp" standard per una stampa veloce e non particolarmente costosa in bianco e nero. Il nome tradizionale per una coda standard è `lp`.
- Una configurazione "color" o una coda per stampe a colori.

I principi della configurazione della stampante con YaST

Il modulo di configurazione della stampante di YaST può essere richiamato non solo attraverso i menu, ma anche dall'utente `root` direttamente dalla riga di comando con `yast2 printer`. Con `yast2 printer .nodetection` potete evitare il rilevamento automatico della stampante. Vedi a riguardo in particolar modo la sezione *Porte parallele* a pagina 139.

Non ogni stampante può essere configurata per entrambi i sistemi di stampa. Alcuni tipi di configurazione sono dunque supportati o solo da CUPS o solo da LPRng/lpdfilter, il modulo di configurazione della stampante di YaST ve lo indicherà.

Passare da CUPS e LPRng/lpdfilter è facile grazie ad un sottomenu della configurazione della stampante di YaST.

Con la configurazione della stampante di YaST potete scegliere tra i seguenti sistema di stampa o passare dall'uno all'altro:

CUPS come server (default nella installazione standard) Con una stampante collegata in locale, CUPS deve girare come server. Se non viene impostata alcuna coda locale tramite YaST, il demone CUPS "cupsd" non verrà lanciato automaticamente. Se cupsd deve venir eseguito comunque, si dovrà abilitare il servizio 'cups' (normalmente per i runlevel 3 e 5) – vedi la sezione *Configurazione rapida di un client* a pagina 192. In particolar modo vengono installati per questo sistema di stampa i seguenti pacchetti :

- Il pacchetto `cups-libs`
- Il pacchetto `cups-client`
- Il pacchetto `cups`
- Il pacchetto `cups-drivers`
- Il pacchetto `cups-drivers-stp`

CUPS esclusivamente come client Se nella rete locale vi è un server di rete CUPS, e se si intende stampare solo attraverso le sue code, è sufficiente che CUPS giri solo come client. Dovete solo indicare il server di rete CUPS. A tal fine bastano i seguenti pacchetti:

- Il pacchetto `cups-libs`
- Il pacchetto `cups-client`

LPRng

- Se volete usare il sistema di stampa LPRng/lpdfilter
- Se nella rete vi è solo un server LPD (vedi sezione *Terminologia* a pagina 191) e si intende stampare attraverso la sua coda – vedi la sezione *Configurazione rapida di un client* a pagina 192.

In questo caso installate i pacchetti:

- Il pacchetto `lprng`
- Il pacchetto `lpdfilter`

Il pacchetto `cups-client` e il pacchetto `lprng` si escludono a vicenda e non possono essere installati insieme. Il pacchetto `cups-libs` deve essere sempre installato, poiché alcuni programmi (per esempio Samba) hanno un link che punta a librerie CUPS.

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

- Il pacchetto `ghostscript-library`

- Il pacchetto `ghostscript-fonts-std`
- Il pacchetto `ghostscript-x11`
- Il pacchetto `libgimpprint`
- Il pacchetto `a2ps`
- Il pacchetto `file`

Il modulo per la configurazione della stampante di YaST vi mostra il tipo di configurazione che è stata generata. Dato che la configurazione viene generata effettivamente solo dopo aver concluso il processo di configurazione della stampante YaST, eseguite una verifica riavviando la configurazione della stampante eseguita con YaST.

Nella configurazione della stampante di YaST si distingue nettamente tra code create con YaST (code YaST), e quelle non create con YaST (code non-YaST). Quest'ultime non possono essere modificate con YaST. Dei conflitti si verificano solo nel caso vi siano dei nomi identici. Quando si elabora una coda di stampa si può scegliere se la configurazione della coda stessa debba venir eseguita con YaST o meno. Trasformando una coda YaST in una non YaST, si possono apportare delle modifiche (senza ricorrere a YaST), senza che vengano sovrascritte da YaST. E' possibile anche l'inverso: trasformare una coda non YaST in una coda di stampa YaST e sovrascriverne la configurazione con una configurazione YaST.

Configurazione automatica

A seconda della misura in cui YaST rivela automaticamente l'hardware e in qual misura 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 premesse:

- 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 deve 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 deve ricorrere a dati di configurazione non esplicitamente supportati dal produttore, e così non è possibile garantire il funzionamento per ogni immissione fatta.

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

Configurazione manuale

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

La 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 fare delle impostazioni.
- 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.

  `/dev/lp0` è la prima porta parallela
  `/dev/usb/lp0` è la porta per una stampante USB

  Configurando manualmente si deve scegliere la porta. In questi casi va assolutamente eseguito una prova di stampa con 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 (esadecimale)
  - L'interrupt non è rilevante
  - Modo `Normal`, `SPP` o `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 inseriti nel seguente modo: `0x378,0x278`. Vedi a riguardo in particolare la sezione *Porte parallele* a pagina 139.

Il nome della coda Dato che spesso quando intendete stampare dovete indicare il nome della coda, usate solo nomi brevi composti da minuscole ed eventualmente cifre.

Con il sistema di stampa LPRng/lpdfilter sussistono le particolari possibilità di configurazione riportate di seguito:

- Per casi particolari potete settare una cosiddetta coda `raw` ovvero grezza. Nella coda `raw` il filtro della stampante non converte i dati da stampare, essi vengono inviati direttamente nello stato grezzo alla stampante. Per questo motivo, se utilizzate una coda `raw` i dati da stampare devono essere già disponibili nel linguaggio della stampante.
- Potete impostare la coda con o senza formfeed (avanzamento di modulo per far avanzare i fogli uno alla volta), ciò dipende dal fatto se lo spooler innesca in modo esplicito un avanzamento di modulo dopo ogni processo di stampa, così da emettere anche l'ultimo foglio dell'incarico. Normalmente se ne occupa il driver Ghostscript, allora non serve indicare esplicitamente alcun avanzamento.

Il driver Ghostscript e il 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, adatta al modello della stampante – cioè 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.

Dato che il driver Ghostscript genera dati 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 e prima ancora delle impostazioni di driver adatte. E' qui vengono che vengono impostate le caratteristiche e le differenze nei risultati tra le diverse configurazioni di una stampante.

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 – per esempio

- 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 del driver, le potete modificare in una maschera a parte. Le voci di menu indentate indicano il nesso tra valore selezionato e le possibilità offerte dalla sottoselezione. Non tutte le combinazioni di impostazioni 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 una prova di stampa con YaST. Se questo tentativo non dovesse produrre il risultato atteso (per esempio tanti fogli quasi vuoti), potete fermare il processo 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 i fogli in fase di stampa vengano emessi.

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 un "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: se concludere il processo di stampa o meno; se la coda debba accettare incarichi di stampa o meno.
- Pagine con banner o frontespizi: se e quali pagine con banner debbano essere stampate prima della stampa vera e propria, e se e quando le pagine banner devono essere stampate dopo il processo vero e proprio.

Il sistema di stampa LPRng/lpdfilter offre le seguenti particolari impostazioni valide per ogni 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 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 sorgenti di PostScript).
- La codificazione nazionale riguarda la raffigurazione dei caratteri speciali nella stampa di testi ASCII e testo semplice nelle pagine HTML di Netscape.

Configurazione per applicativi

Gli applicativi utilizzano code esistenti come nel caso del processo di stampa dalla riga di comando. Per tale motivo negli applicativi non viene configurata la stampante ma la coda esistente.

Stampare dalla riga di comando

Dalla riga di comando potete stampare attraverso il comando `lpr -Plp NOMEFILE`, dove `NOMEFILE` va sostituito con il nome del file da stampare. In questo caso viene usata la coda standard `lp`. Attraverso l'opzione `-P` si può determinare esplicitamente la coda. Con `lpr -Pcolor NOMEFILE` viene usata per esempio la coda `color`.

Con il sistema di stampa LPRng/lpdfilter

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

Configurazione manuale delle porte di una stampante locale

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 YaST viene descritta nella sezione *Configurazione manuale* a pagina 136, seguono 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 poter fare funzionare *contemporaneamente* diversi dispositivi collegati a catena (per esempio 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 (ingl. *Kernel Module Loader*), non appena si accede per la prima volta ad un file di dispositivo (per esempio `/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 questo non funziona, e si può verificare un immediato blocco del sistema. A questo punto bisogna configurare i parametri corretti per il modulo `parport_pc` a mano. Per tale motivo, come descritto nella sezione *Configurare la stampante con YaST* a pagina 133, con YaST si lascia evitare il rilevamento automatico della stampante.

Configurazione manuale della porta parallela

La porta parallela `/dev/lp0` viene configurata attraverso la registrazione in `/etc/modules.conf` (file 4).

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

file 4: */etc/modules.conf: prima porta parallela*

Accanto ad `io` si vede l'indirizzo IO della porta parallela.

Accanto ad `irq` vi è `none` quale preimpostazione per il funzionamento nella modalità "polling" oppure l'interrupt della porta parallela. Il polling è meno problematico dell'interrupt, dal momento che si evitano 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 è in esecuzione 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 con

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

file 5: */etc/modules.conf: modalità interrupt per la prima porta parallela*

la modalità interrupt può essere attivata. Prima di attivare la modalità interrupt, con

```
terra:~ #  cat /proc/interrupts
```

bisogna determinare quali interrupt sono già utilizzati; qui vengono mostrati solo gli interrupt che vengono utilizzati al momento, il che può variare dall'hardware in uso. L'interrupt per la porta parallela non può essere già assegnato. Se non siete certi, utilizzate la modalità polling.

Configurazione di ulteriori porte parallele

Una seconda interfaccia parallela `/dev/lp1` solitamente indirizzabile tramite l'indirizzo IO standard 278 (esadecimale) (impostabile, ad esempio, tramite jumper su una scheda di interfaccia ISA), può essere configurata anche in `/etc/modules.conf` (file 6).

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378,0x278 irq=none,none
```

file 6: */etc/modules.conf: due porte parallele*

Schede di espansione speciali: schede ISA-PnP e PCI

Innanzitutto, se non avete fatto già, dovete rilevare l'indirizzo IO della porta parallela aggiuntiva.

Schede ISA PnP Se potete impostare con queste schede un valore fisso per l'indirizzo IO e, eventualmente, per l'interrupt ed il modo di funzionamento (per esempio, tramite jumper), fatelo.

Altrimenti i valori per l'indirizzo IO, interrupt e modo della scheda ISA PnP vengono impostati all'avvio di Linux. Quali valori sono stati impostati, lo si può vedere nei messaggi di boot di Linux (nel file `/var/log/boot.msg`) oppure tramite il comando `pnpdump` (il pacchetto `isapnp`)

Schede PCI Quali indirizzi IO e quale interrupt siano adatti per una scheda PCI, si può appurare con il seguente comando (vd. l'output *Schede di espansione speciali: schede ISA-PnP e PCI* in questa pagina):

```
terra:~ #  /sbin/lspci -v


00:0a.0 Parallel controller: ...
        ... IRQ 10
        I/O ports at b400
        I/O ports at b000
        I/O ports at a800
        I/O ports at a400
```

output 11: *Estratto di* `lspci -v` *per una scheda di interfaccia PCI*

Rispettivamente due indirizzi IO con un intervallo di 400 (esadecimale) appartengono entrambi ad una porta parallela – nel nostro esempio il valore `b000` e `b400` fanno riferimento ad una porta mentre `a400` e `a800` all'altra. Eventualmente va testato con quale dei due indirizzi funzioni effettivamente la scheda; i valori della configurazione in `/etc/modules.conf` saranno simili al file 7.

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378,0xb400,0xa800 irq=none,none,none
```

file 7: */etc/modules.conf: scheda PCI con due porte parallele*

Attivazione e test di un'interfaccia parallela

Dopo aver riavviato il sistema potete utilizzare l'interfaccia parallela.

Invece di eseguire un reboot del sistema, è sufficiente aggiornare, come utente `root`, la lista delle dipendenze dei moduli del kernel scaricando i moduli del kernel che riguardano l'interfaccia parallela...

```
terra:~ #  depmod -a 2>/dev/null
terra:~ #  rmmod lp
terra:~ #  rmmod parport_pc
terra:~ #  rmmod parport
```

...e ricaricarli con:

```
terra:~ #  modprobe parport
terra:~ #  modprobe parport_pc
terra:~ #  modprobe lp
```

Se la stampante è in grado di stampare testi ASCII, come `root` date il comando

```
terra:~ #  echo -en "\rHello\r\f" >/dev/lp0
```

per stampare una pagina con la parola `Hello`.

Nell'esempio la parola `Hello` mostra alla inizio e alla fine il simbolo ASCII \r, che codifica il ritorno di carrello ed è seguita dal simbolo ASCII \f, che codifica un avanzamento di modulo spesso abbreviato con FF (per formfeed).

Per una seconda interfaccia parallela, selezionate `/dev/lp1`; per una terza, selezionate `/dev/lp2`.

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 menù 'PNP AND PCI SETUP' su `Enabled`. A seconda della versione BIOS potete incontrare anche designazioni differenti.

Immettendo, come utente `root` :

```
terra:~ #  echo -en "\rHello\r\f" >/dev/usb/lp0
```

verificate se la stampante USB è indirizzabile.

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

Alcune stampanti necessitano una sequenza di controllo speciale, prima di accettare dei dati tramite la porta USB. Il seguente comando invia la sequenza di controllo adatta a stampanti USB Epson Stylus Color (immettete il comando in una sola riga senza spazi o ritorni a capo):

```
echo -en "\x0\x0\x0\x1b\x01\x40\x45\x4a\x4c
\x20\x31\x32\x38\x34\x2e\x34\x0a\x40\x45\x4a\x4c\x20
\x20\x20\x20\x20\x0a" >/dev/usb/lp0
```

Ulteriori informazioni le trovate anche nella banca dati di supporto effettuando una ricerca con le parole chiave “Epson” e “usb”.

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

```
terra:~ #  cat /proc/bus/usb/devices
```

Se non vengono indicati né il produttore né il nome del 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 così 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 non risponda più (per esempio, se si stacca lo spinotto USB). Di solito dovrebbe bastare immettere questi comandi per riavviare il sistema USB:

```
terra:~ #  rchotplug stop
terra:~ #  rchotplug start
```

Altrimenti, terminate tutti i processi che accedono a `/dev/usb/lp0` e scaricate e ricaricate i moduli del kernel che riguardano la stampante USB. Con `lsmod` controllate prima quali moduli USB siano stati caricati (se `usb-uhci` o `usb-ohci` o `uhci`) e se ci siano ulteriori dipendenze di moduli, ad esempio la segnalazione

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

indica che il modulo `usbcore` è ancora necessario ai moduli `printer` ed `usb-uhci`. Perciò, in questo caso, prima del modulo `usbcore`, devono venire scaricati i moduli `printer` ed `usb-uhci`. Immettete come `root` i seguenti comandi (al posto di `usb-uhci` a secondo del sistema anche `uhci` o `usb-ohci`):

```
terra:~ #  fuser -k /dev/usb/lp0
terra:~ #  rchotplug stop
terra:~ #  rmmod printer
terra:~ #  rmmod usb-uhci
terra:~ #  umount usbdevfs
terra:~ #  rmmod usbcore
terra:~ #  modprobe usbcore
terra:~ #  mount usbdevfs
terra:~ #  modprobe usb-uhci
terra:~ #  modprobe printer
terra:~ #  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 quale dispositivo `/dev/usb/lp0`. La seconda stampante USB rilevata, è indirizzabile tramite `/dev/usb/lp1`. Alcuni modelli di stampante vengono rilevati automaticamente anche quando sono spente; ciò è dovuto al fatto che alcune stampanti possono essere rilevate, anche se sono spente, tramite il collegamento USB. Per evitare di perdere la visione di insieme per quanto riguarda i dispositivi USB, prima di avviare Linux accendete tutte le stampanti USB e possibilmente mantenetele tali per tutto il tempo in cui il sistema è in esecuzione.

Interfaccia IrDA della stampante

Tramite l' interfaccia ad infrarossi viene emula una porta parallela. Il driver del kernel mette a disposizione un'interfaccia parallela simulata sotto `/dev/irlpt0`. Una stampante dunque viene indirizzata alla stregua di una stampante collegata alla porta parallela con la sola differenza che al posto di `/dev/lp0` abbiamo `/dev/irlpt0`.

Provate se la stampante IrDA è indirizzabile immettendo come utente root:

```
terra:~ #  echo -en "\rHello\r\f" >/dev/irlpt0
```

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

Ad ogni caso la stampante dovrebbe comparire nell'output del seguente comando:

```
terra:~ #  irdadump
```

Se il comando irdadump non esiste, allora bisogna installare il pacchetto `irda`, altrimenti la stampante non è indirizzabile.

Se non viene indicato proprio niente, allora probabilmente il servizio di sistema IrDA non è stato inizializzato, dato che non viene inizializzato automaticamente all'avvio. Con

```
terra:~ #  rcirda start
terra:~ #  rcirda stop
```

potete avviare e fermare il servizio di sistema IrDA.

Interfaccia seriale

Il funzionamento di una stampante collegata ad un'interfaccia seriale in combinazione con lo spooler LPRng 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 pagina di manuale di `printcap` (`man printcap`). Nella banca dati di supporto trovate ulteriori informazioni avviando una ricerca immettendo il termine serial.

La configurazione manuale di LPRng/lpdfilter

Di solito il sistema di stampa viene configurato con YaST, come descritto nella sezione *Configurare la stampante con YaST* a pagina 133.

Inoltre per il sistema di stampa LPRng/lpdfilter esiste il programma lprsetup basato sulla riga di comando.

Quando una stampante viene configurata con YaST, vengono raccolte le informazioni necessarie e richiamato lprsetup con le opzioni necessarie per configurare il sistema di stampa LPRng/lpdfilter.

Il programma lprsetup è stato ideato come tool ovvero strumento di configurazione per utenti "esperti". A differenza di YaST, lprsetup non aiuta l'utente con delle proposta a stabilire i valori giusti per le singole opzioni.

Con `lprsetup -help` vengono elencate e descritte le opzioni possibili, e ulteriori informazioni sono reperibili nella pagina di manuale di `lprsetup` (`man lprsetup`) o nella pagina di manuale di `lpdfilter` (`man lpdfilter`).

Per avere informazioni su driver Ghostscript e parametri specifici del driver vedi la sezione *Determinare il driver adatto alla stampante* a pagina 129 e *Su Ghostscript* a pagina 178.

Lo spooler di stampa LPRng/lpdfilter

Come spooler del sistema di stampa LPRng/lpdfilter viene utilizzato il pacchetto `lprng`.

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

```
terra:~ #  rclpd start
terra:~ #  rclpd stop
```

I file di configurazione per l'LPRng sono:

/etc/printcap Configurazione delle singole code

/etc/lpd.conf Configurazione complessiva dello spooler

/etc/lpd.perms Configurazione dei permessi di accesso

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

Lo spooler di stampa rivela all'avvio, basandosi sulle registrazioni in `/etc/printcap`, le code definite. Il suo compito è quello di amministrare l'esecuzione degli incarichi in coda, inoltre:

- Amministra le code locali, invia i file con i dati di un incarico eventualmente al filtro della stampante ed in seguito direttamente alla stampante o ad una altra coda.
- Registra la successione degli incarichi nella coda.
- Controlla lo stato delle code e della stampante e ne riferisce su richiesta.
- Sta in ascolto sulla porta 515 per accettare o eventualmente rifiutare incarichi di stampa provenienti da computer remoti destinate alle code locali.
- Inoltra gli incarichi di stampa a spooler di computer remoti (dunque la porta 515 del computer remoto).

Per i dettagli sullo spooler LPRng leggete *LPRng-Howto* sotto
`file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html`
La pagina di manuale di `printcap` (`man printcap`) e la pagina di manuale di `lpd` (`man lpd`).

Tool della riga di comando per LPRng

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

Per code locali

Generare incarichi di stampa

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

Normalmente si stampa con

```
tux@terra:~ >  lpr -P⟨coda⟩ ⟨file⟩
```

Ommettendo l'opzione `-P`⟨*coda*⟩, di default si assume il contenuto della variabile di ambiente `PRINTER`. Questo vale anche per i comandi `lpq` e `lprm` – vedi la pagina di manuale di `lpr` (`man lpr`), la pagina di manuale di `lpq`

(`man lpq`) e la pagina di manuale di `lprm` (`man lprm`). La variabile di ambiente `PRINTER` viene impostata automaticamente al login, e può essere visualizzata con il comando `echo $PRINTER` e con

```
tux@terra:~ >  export PRINTER=⟨coda⟩
```

venir impostata su un'(altra) coda.

Mostrare lo stato

```
tux@terra:~ >  lpq -P⟨coda⟩
```

mostra gli incarichi di stampa della coda indicata. Se per lo spooler LPRng immettete come coda `all`, vengono elencati tutti gli incarichi di tutte le code.

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

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

Per ulteriori informazioni vedi sotto la sezione *Mostra lo stato di code remote*, la pagina di manuale di `lpq` (`man lpq`) ed infine `file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#LPQ` nell' *LPRng-Howto*.

Cancellare incarichi di stampa

```
tux@terra:~ >  lprm -P⟨coda⟩ ⟨numero dell'incarico⟩
```

cancella l'incarico specificato dalla coda indicata se l'incarico appartiene all'utente che ha immesso il comando `lprm`. L'incarico appartiene all'utente che ha inviato l'incarico. Questo utente si lascia identificare con il comando `lpq` che mostra anche il numero dell'incarico.

Con il comando

```
terra:~ #  lprm -Pall all
```

vengono cancellati tutti gli incarichi di tutte le code per i quali ha il permesso l'utente che ha immesso il comando `lprm`. L'utente `root` può cancellare ogni incarico (anche in tutte le code).

Ulteriori informazioni nella pagina di manuale di `lprm` (`man lprm`) e sotto `file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#LPRM` nell'*LPRng-Howto*.

Controllo delle code

`tux@terra:~ >` **`lpc option`** ⟨*coda*⟩

mostra lo stato delle code indicate e consente di modificarle.

Le opzioni principali sono:

`help` dà un sommario delle opzioni.

`status` ⟨*coda*⟩ emette un resoconto sullo stato.

`disable` ⟨*coda*⟩ rifiuta nuovi incarichi.

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

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

`start` ⟨*coda*⟩ riprende con lo stampare degli incarichi della coda.

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

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

`abort` ⟨*coda*⟩ 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 (`up`).

Per intervenire sulle code dovete agire da `root`.

Potete immettere questi comandi direttamente nella riga di comando (per esempio `lpc status all`), o richiamate `lpc` senza parametri che viene inizializzato nel modo dialogo e si presenta con il prompt lpc> aspettandosi l'immissione delle opzioni riportate sopra. Con `quit` o `exit` uscite dal dialogo.

Se per esempio `lpc status all` 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 coda `lp` è abilitata e contiene due incarichi, di cui uno si trova in fase di stampa. La coda `color` è disabilitata. Nella coda di `laser`, per esempio per motivi di manutenzione della stampante, è momentaneamente disabilitata la stampa, ma è tuttavia possibile continuare a generare degli incarichi che vengono raccolti nella coda (nel nostro esempio: 8).

Ulteriori informazioni si trovano nella pagina di manuale di `lpc` (`man lpc`) e sotto
`file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#LPC`
nella *LPRng-Howto*.

Gestire code remote

Qui dovete sostituire `print-server` con il nome o l'indirizzo IP del server di stampa, e ⟨*coda*⟩ deve essere una coda sul server di stampa.

Generare incarichi di stampa

Con lo spooler LPRng si può accedere a coda remote con il comando `lpr`:

```
tux@terra:~ >  lpr -P⟨coda⟩@server di stampa ⟨file⟩
```

La premessa è che il server di stampa sia stato configurato in modo che sia possibile utilizzare le sue code, cosa consentita di default con LPRng.

Mostrare lo stato

Con i comandi

```
tux@terra:~ >  lpq -P⟨coda⟩@server di stampa
tux@terra:~ >  lpq -s -P⟨coda⟩@server di stampa
tux@terra:~ >  lpq -l -P⟨coda⟩@server di stampa
tux@terra:~ >  lpq -L -P⟨coda⟩@server di stampa
```

e

```
tux@terra:~ >  lpc status ⟨coda⟩@server di stampa
tux@terra:~ >  lpc status all@server di stampa
```

potete vedere lo stato di code remote.

Soprattutto con `lpq -s -Pall@server di stampa` o `lpc status all@print-server` possono venire rilevati i nomi di

tutte le code di stampa sul server di stampa, se utilizzate LPRng anche sul server di stampa.

Se non è possibile stampare tramite code remote, date una occhiata allo stato delle code remote per avere delle utili indicazioni.

Con `lpq -L -P`⟨*coda*⟩`@server di stampa` può essere visualizzato un rapporto sullo stato ai fini della diagnosi da remoto, sempre se sul server di stampa utilizzate LPRng.

Cancellare incarichi di stampa

Con i comandi

```
tux@terra:~ >  lprm -P⟨coda⟩@server di stampa ⟨numero
     dell'incarico⟩
tux@terra:~ >  lprm -P⟨coda⟩@server di stampa all
tux@terra:~ >  lprm -Pall@server di stampa all
```

potrete cancellare tutti gli incarichi su code remote che avete generato voi. In particolare, `root` non ha alcun tipo di privileggi nei confronti di code remote.

`all` funziona solo se anche sul server di stampa gira LPRng.

Eliminare disfunzioni in LPRng con i comandi descritti sopra

Gli incarichi di stampa permangono nella coda anche se si spegne il computer durante il processo di stampa e riavviate poi Linux – un incarico di stampa contenente degli errori va rimosso dalla coda tramite i comandi riportati sopra.

Se per esempio si verifica un guasto nel processo di comunicazione tra computer e stampante, la stampante non è in grado di elaborare in modo corretto i dati che le sono stati inviati, e come risultato emette innumerevoli fogli pieni di 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 solo dopo essere stato inviato completamente alla stampante, lo si ritroverà nella maggior parte dei casi ancora nella coda. Controllate con `lpq` o `lpc status` quale incarico di quale coda è attualmente in fase 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. Tutti processi che accedono ancora alla stampante vengono terminati con il comando `fuser -k /dev/lp0` nel caso di 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 la carta nell'apposito cassetto e accendete la stampante.

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 *Il debug di lpdfilter* a pagina 161.

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

2. Viene determinato il tipo di dati da stampare. Con `/usr/lib/lpdfilter/bin/guess`, viene applicato il comando `file` ai dati da stampare. Con il suo output e sulla base dei valori nel file `/etc/lpdfilter/types`, viene fissato il tipo di dati da stampare.

   - Se si tratta di una coda `ascii`, il filtro viene costretto a trattare i dati da stampare come caratteri ASCII.
   - Se non si tratta di una coda `ascii`, il filtro cerca di determinare automaticamente il tipo di dati da stampare.

3. A seconda del tipo dei dati e di coda, avviene ora il processo di conversione dei dati nei dati da inviare alla stampante:

   - 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*⟩/conf lo prevedono, essi possono anche venire ricodificati con recode. Nel caso di una coda raw (grezza ovvero senza lpdfilter), cancellate per la coda in questione, la riga :if=/usr/lib/lpdfilter/bin/if:\ in /etc/printcap.

- Se non si tratta di una coda grezza :
  (a) Se i dati da stampare non sono PostScript, lo diventeranno richiamando /usr/lib/lpdfilter/filter/tipo2ps (laddove tipo va sostituito con il tipo dei dati da stampare). I testi ASCII, in particolare, vengono tradotti in PostScript con il programma a2ps in base a /usr/lib/lpdfilter/filter/ascii2ps e secondo la codificazione della lingua configurata per la coda. In questo modo, tutti i caratteri speciali potranno essere stampati correttamente anche nel semplice formato di testo; vd. anche la pagina di manuale di a2ps (man a2ps).
  (b) I dati PostScript possono anche essere riformattati, a condizione che, in /etc/lpdfilter/⟨*coda*⟩/pre vi sia uno script adatto (laddove coda va sostituito con il nome della coda).
  (c) Anche i dati PostScript si convertire in un altro linguaggio.
    ▷ Se avete una stampante PostScript, i dati in PostScript vengono inviati direttamente ad essa (o ad un'altra coda). Eventualmente vengono richiamate inoltre le funzioni bash "duplex" e "tray", come definite in /usr/lib/lpdfilter/global/functions, per permettere la stampa duplex o la scelta del cassetto dei fogli tramite comandi PostScript (a condizione che la stampante PostScript supporti questi comandi).
    ▷ Se non avete una stampante PostScript, verrà utilizzato Ghostscript con un driver adatto al linguaggio del modello della stampante, per poter produrre i dati da inviare alla stampante (o ad un'altra coda).
    Troverete i parametri per Ghostscript in /etc/printcap nella riga cm o nel file /etc/lpdfilter/⟨*coda*⟩/upp (sostituite coda con il nome della coda).
    L'output di Ghostscript può essere anche riformattato, a condizione che /etc/lpdfilter/⟨*coda*⟩/post contenga uno script adatto (sostituite coda con il nome della coda).
  (d) I dati da stampare vengono inviati alla stampante (o ad un'altra coda). Oltre ai dati potete inviare anche determinate sequenze di controllo, se le avete impostate in /etc/lpdfilter/⟨*coda*⟩/conf.

La configurazione dell' lpdfilter

Normalmente il sistema di stampa viene configurato con YaST come descritto nella sezione *Configurare la stampante con YaST* a pagina 133, ed in particolar modo viene configurato l'lpdfilter.

Per impostazioni speciali dovete adattare manualmente i file di configurazione del filtro della stampante.

Ogni coda ha il proprio file di configurazione `/etc/lpdfilter/`⟨*coda*⟩`/conf` (sostituite `coda` con il nome effettivo della coda) che contiene inoltre informazioni su ogni opzione.

Personalizzare l'lpdfilter

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

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

2. I dati PostScript possono anche essere riformattati ancora una volta, a condizione che in `/etc/lpdfilter/`⟨*coda*⟩`/pre` vi sia uno script adatto. Potete caricare anche dei vostri cosiddetti preload PostScript tramite uno script adatto. Questo script raccoglie i dati da stampare tramite `stdin` e li emette in formato PostScript tramite `stdout`. Applicazioni per riformattare dati PostScript si trovano nel pacchetto `psutils`. In particolar modo pstops consente una ampia riformattazione; vedi a riguardo la pagina di manuale di `pstops` (`man pstops`).

3. Parametri speciali per Ghostscript: durante la configurazione con YaST, vengono memorizzati i parametri di chiamata di Ghostscript nel file `/etc/lpdfilter/`⟨*coda*⟩`/upp` (sostituite `coda` con il nome della coda). In questo file, potrete inserire manualmente anche dei parametri speciali per Ghostscript. Vd. anche il paragrafo *Su Ghostscript* a pagina 178.

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

Un esempio, a prescindere dell'hardware

Partiamo dal presupposto che vi sia una coda `test`, attraverso la quale si debba stampare un testo ASCII con righe numerate e che un foglio debba contenere due pagine ridotte. In questo caso, si possono creare i seguenti script: `/etc/lpdfilter/test/ascii2ps` ed `/etc/lpdfilter/test/pre`:

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

file 8: */etc/lpdfilter/test/ascii2ps: convertire ASCII in PostScript*

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

file 9: */etc/lpdfilter/test/pre: riformattare PostScript*

Questi script devono essere eseguibili per ogni utente, ricorrete a tal fine al comando `chmod`:

```
terra:~ #  chmod -v a+rx /etc/lpdfilter/test/ascii2ps
terra:~ #  chmod -v a+rx /etc/lpdfilter/test/pre
```

`pstops` funziona solo per file PostScript creati in modo da consentire la riformattazione (cosa che di solito dovrebbe essere così).

Usare preload PostScript personalizzati

I preload PostScript sono dei piccoli file PostScript che contengono comandi PostScript speciali che precedono i dati da stampare veri e propri, per poter inizializzare una stampante PostScript o Ghostscript nel modo desiderato.

Normalmente, i preload PostScript vengono usati per abilitare la stampa duplex su stampanti PostScript o per abilitare determinati cassetti della carta oppure per impostare i margini e la correzione gamma.

Il presupposto è che la stampante PostScript o Ghostscript riesca ad elaborare i comandi PostScript descritti di seguito (Ghostscript non reagisce a comandi concernenti la stampa duplex o la scelta del cassetto dei fogli). Supponiamo che la coda si chiami `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`:

```
%!PS
statusdict /setduplexmode known
{statusdict begin true setduplexmode end} if {} pop
```

file 10: */etc/lpdfilter/test/duplexon.ps: attivare la stampa duplex*

```
%!PS
statusdict /setduplexmode known
{statusdict begin false setduplexmode end} if {} pop
```

file 11: */etc/lpdfilter/test/duplexoff.ps: disattivare la stampa duplex*

Selezione del cassetto della carta Per attivare il cassetto della carta standard con la cifra 0 o il cassetto per esempio con la cifra 2, potete creare i seguenti file `/etc/lpdfilter/test/tray0.ps` e `/etc/lpdfilter/test/tray2.ps`:

```
%!PS
statusdict /setpapertray known
{statusdict begin 0 setpapertray end} if {} pop
```

file 12: */etc/lpdfilter/test/tray0.ps: attivare il cassetto 0*

```
%!PS
statusdict /setpapertray known
{statusdict begin 2 setpapertray end} if {} pop
```

file 13: */etc/lpdfilter/test/tray2.ps: attivare il cassetto 2*

Margini Per impostare i margini, potete creare il seguente file `/etc/lpdfilter/test/margin.ps`:

```
%!PS
<<
/.HWMargins [left bottom right top]
/PageSize [width height]
/Margins [left-offset top-offset]
>>
setpagedevice
```

file 14: */etc/lpdfilter/test/margin.ps: impostare i margini*

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 del testo stampato sul foglio, basta il file `/etc/lpdfilter/test/offset.ps`

```
%!PS
<< /Margins [left-offset top-offset] >> setpagedevice
```

file 15: */etc/lpdfilter/test/offset.ps: posizione dello stampato*

Correzione gamma Per intervenire sul bilanciamento dei colori, create i file `/etc/lpdfilter/test/cmyk.ps` ed `/etc/lpdfilter/test/rgb.ps`:

```
%!PS
{cyan exp} {magenta exp} {yellow exp} {black exp} \
setcolortransfer
```

file 16: */etc/lpdfilter/test/cmyk.ps: correzione gamma CMYK*

```
%!PS
{red exp} {green exp} {blue exp} currenttransfer \
setcolortransfer
```

file 17: */etc/lpdfilter/test/rgb.ps: correzione gamma RGB*

Il modello dei colori (CMYK o RGB) deve adattarsi alla vostra stampante. I valori da impostare per `cyan`, `magenta`, `yellow`, `black`, `red`, `green` e `blue`, vanno determinati tramite dei test. Di solito si tratta di valori tra `0.001` e `0.999`.

Potete verificare l'effetto dei file sovrariportati tramite l'interfaccia grafica allo schermo; senza correzione gamma:

```
terra:~ #  gs -r60 \
    /usr/share/doc/packages/ghostscript/examples/colorcir.ps
```

Con correzione gamma:

```
terra:~ #  gs -r60 /etc/lpdfilter/test/cmyk.ps \
    /usr/share/doc/packages/ghostscript/examples/colorcir.ps
terra:~ #  gs -r60 /etc/lpdfilter/test/rgb.ps \
    /usr/share/doc/packages/ghostscript/examples/colorcir.ps
```

Il comando va inserito in una sola riga e senza (ingl. *backslash*, `'\'`).

Per terminare il test, premere Ctrl + c.

Resettare la stampante Per riportare la stampante allo stato originario potete creare il seguente file `/etc/lpdfilter/test/reset.ps`:

```
%!PS
serverdict begin 0 exitserver
```

file 18: */etc/lpdfilter/test/reset.ps: resettare la stampante*

Per attivare un preload PostScript potete creare il seguente script `/etc/lpdfilter/test/pre`:

```
#!/bin/bash
cat /etc/lpdfilter/test/preload.ps -
```

file 19: */etc/lpdfilter/test/pre: caricare preload PostScript*

Sostituite `preload.ps` con il nome del file preload del caso. Lo script deve essere eseguibile e leggibile per tutti gli utenti, ciò viene realizzato con il comando `chmod`:

```
terra:~ #  chmod -v a+rx /etc/lpdfilter/test/pre
terra:~ #  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 creare il seguente script `/etc/lpdfilter/test/pre`:

```
%

#!/bin/bash
cat /etc/lpdfilter/test/preload.ps - /etc/lpdfilter/test/reset.ps
```

file 20: */etc/lpdfilter/test/pre: preload e reset PostScript*

Esempio di configurazione di una stampante GDI

Configuriamo adesso una coda di stampa `gdi` per una stampante GDI.

Questo tipo di stampante normalmente non è compatibile con Linux, vd. paragrafo precedente *Stampanti GDI* a pagina 130.

Tuttavia, per alcune stampanti GDI esistono degli speciali programmi driver, che normalmente vengono utilizzati come complemento per Ghostscript, i quali convertono l'output di Ghostscript nel formato adatto alla stampante. Questi programmi driver comunque spesso comportano delle restrizioni per quel che riguarda il risultato emesso dalla stampante – consentendo per esempio la stampa solo in bianco e nero.

Ghostscript ed i programmi driver collaborano come descritto di seguito: (cfr. il paragrafo *Su Ghostscript* a pagina 178.)

1. I dati PostScript vengono risolti da Ghostscript in una matrice di tanti punti. Un driver Ghostscript emette i dati della matrice in un formato e con una risoluzione adatta al programma driver.
2. Il programma driver converte i dati della matrice nel formato della stampante.

Si parte qui dal presupposto che disponete di un programma driver per la stampante adatto alla vostra versione di SuSE Linux o che possa essere scaricato dall'Internet. Si presuppone inoltre che il programma driver funzioni come descritto sopra, e che sappiate usare in Unix per esempio archivi `.zip` o `.tar.gz` oppure pacchetti `.rpm`. Dopo aver decompresso un tale archivio, troverete delle istruzioni di installazione in file di nome `README` o `INSTALL` oppure in una sottodirectory di nome `doc`. Nel caso di archivi `.tar.gz`, il programma driver vero e proprio deve essere compilato ed installato.

Nel seguente esempio presupponiamo che:

- Il programma driver sia `/usr/local/bin/printerdriver`.
- Il driver Ghostscript `pbmraw` con una risoluzione di 600 dpi.
- La stampante sia collegata alla prima interfaccia parallela `/dev/lp0`.

Quale driver Ghostscript e quale risoluzione utilizzare effettivamente viene indicato nella documentazione del programma driver. Per prima cosa, create la coda di stampa `gdi` con lprsetup (come `root`):

```
terra:~ #  lprsetup -add gdi -lprng -device /dev/lp0 \
     -driver pbmraw -dpi 600 -size a4dj -auto -sf
```

Questo comando va scritto in una sola riga senza backslash `'\'`.

Quindi, generate il seguente script `/etc/lpdfilter/gdi/post`:

```
#!/bin/bash
/usr/local/bin/printerdriver ⟨parametri_specifici_del_driver⟩
```

file 21: */etc/lpdfilter/gdi/post: chiamata del programma di driver*

Eventualmente inserite 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 della stampante:

```
terra:~ #  chmod -v a+rx /etc/lpdfilter/gdi/post
terra:~ #  rclpd stop
terra:~ #  rclpd start
```

Ora, tutti gli utenti potranno stampare come segue:

```
tux@terra:~ >  lpr -Pgdi ⟨file⟩
```

Il debug di lpdfilter

Per attivare il livello di debug appropriato, eliminate il simbolo di commento # davanti alla riga corrispondente nello script principale `/usr/lib/lpdfilter/bin/if` del filtro della stampante.

```
# DEBUG="off"
# DEBUG="low"
DEBUG="medium"
# DEBUG="high"
```

file 22: */usr/lib/lpdfilter/bin/if: livello di debug*

Con `DEBUG=low`, verrà salvato solo l'output `stderr` di `/usr/lib/lpdfilter/bin/if` in un file `/tmp/lpdfilter.if-$$.XXXXXX` (sostituite a `$$` il numero del processo; a `XXXXXX` sostituite 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-$$.XXXXXX` (laddove `nome` sia il nome dello script lanciato e `$$.XXXXXX` 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` sia una combinazione di cifre casuale ma univoca).

Per mantenere un pò d'ordine, cancellate questi file prima di ogni test con `rm -v /tmp/lpdfilter*`.

Propri filtri di stampante per lo spooler di stampa LPRng

In seguito cercheremo di spiegare i retroscena del processo di stampa sotto Linux servendoci nel nostro esempio di un filtro per stampante che abbiamo creato in precedenza. Per poter spiegare meglio i passaggi cruciali, facciamo un esempio semplice. Per questo si è rinunciato anche ad una descrizione del modo di eliminare errori (debugging) nello script del filtro.

In seguito, si parte dal presupposto che la stampante sia collegata alla prima interfaccia parallela `/dev/lp0`. Un filtro riceve, attraverso lo spooler, i dati da stampare tramite lo standard input. Il filtro della stampante deve trasformare questi dati nel formato della stampante ed emetterli tramite lo standard output. Lo spooler fa sì che quanto viene emesso dal filtro tramite l'emissione standard, arrivi al dispositivo della stampante `/dev/lp0`. Il kernel da parte sua inoltra all'interfaccia da definire (p.e. all'indirizzo IO `0x378`) tutto quello che arriva alla stampante. L'hardware provvede affinché tutto quanto inviato per esempio all'indirizzo IO `0x378`, venga inviato anche alla stampante attraverso l'interfaccia parallela. La stampante interpreta questo flusso di dati e li stampa.

Normalmente, i seguenti comandi possono solo venire eseguiti come utente `root`; questo perché i "normali" utenti non possono accedere direttamente al dispositivo della stampante.

I comandi vengano indicati come segue:

```
terra:~ #  cat file ascii >/dev/lp0
```

Chiaramente `cat file ascii` va sostituito con il nome di un file ASCII vero.

Un semplice esempio del modo fondamentale di funzionamento

Tramite il comando

```
terra:~ #  echo -en "\rHello\r\f" >/dev/lp0
```

non viene attivato alcun spooler o filtro della stampante, poiché viene direttamente indirizzato il device della stampante `/dev/lp0`. In questo modo, solo i caratteri ASCII `'\r'`, `'H'`, `'e'`, `'l'`, `'o'` e `'\r'` e `'\f'` vengono inviati direttamente alla stampante. Il carattere ASCII per il carriage-return (ritorno di carrello) `'\r'` codifica un capoverso ed il carattere ASCII per il form feed (avanzamento del modulo) `'\f'` comporta l'emissione del foglio stampato.

Anche con

```
terra:~ #  cat ascii-file >/dev/lp0
terra:~ #  echo -en "\f" >/dev/lp0
```

non viene abilitato né lo spooler né il filtro della stampante, ancora una volta viene indirizzato direttamente il device della stampante `/dev/lp0`. I caratteri ASCII del file di testo ASCII vengono inviati direttamente alla stampante assieme al carattere ASCII per l'avanzamento del modulo (form feed) che comporta l'emisione anche dell'ultimo foglio dalla stampante.

In Linux, due righe di testo ASCII vengono divise solamente da un carattere di interlinea ASCII (ingl. *line feed*); sotto DOS/Windows due righe di testo ASCII vengono separate da un carattere di interlinea ASCII e da uno per il carriage return (ritorno di carrello).

Se con:

```
terra:~ #  cat /etc/hosts >/dev/lp0
terra:~ #  echo -en "\f" >/dev/lp0
```

si invia direttamente alla stampante un file di testo ASCII `/etc/hosts` si ha normalmente questo risultato

```
first line
          second line
```

poiché la stampante esegue solo un interlinea, ma non esegue il ritorno di carrello in quanto non vi è alcun carattere ASCII per il ritorno di carrello (carriage return).

È però possibile impostare la stampante in modo che questa, con un carattere ASCII per l'interlinea esegua sia un ritorno di linea che un ritorno di carrello.

Con la sequenza di escape `\033&k2G`, le stampanti compatibili con il linguaggio PCL 3 vengono impostate in modo che con un carattere ASCII per l'interlinea venga eseguito sia un ritorno di linea che un ritorno di carrello. Con

```
terra:~ #  echo -en "\033&k2G" >/dev/lp0
```

la sequenza di escape viene inviata alla stampante e alla fine viene stampato il file di testo ASCII con un ritorno a capo corretto.

Probabilmente, gli accenti non verranno stampati correttamente, perché in DOS/Windows la codificazione degli accenti è diversa da Linux e la stampante è normalmente preimpostata per DOS/Windows.

Con

```
terra:~ #  cp ascii-file ascii-file.ibmpc
terra:~ #  recode lat1..ibmpc ascii-file.ibmpc
```

viene prima copiato `ascii-file` verso `ascii-file.ibmpc` e quindi `ascii-file.ibmpc` viene ricodificato per DOS/Windows.

Con

```
terra:~ #  cat ascii-file.ibmpc >/dev/lp0
terra:~ #  echo -en "\f" >/dev/lp0
```

dovrebbero venir stampati correttamente sia il ritorno a capo che gli accenti. Poiché nel file `ascii-file.ibmpc` sia il ritorno a capo che gli accenti sono codificati secondo DOS/Windows, non è più necessaria alcuna speciale sequenza di escape per impostare il ritorno a capo.

Con

```
terra:~ #  cp ascii-file ascii-file.ibmpc
terra:~ #  recode lat1..ibmpc ascii-file.ibmpc
terra:~ #  cat ascii-file.ibmpc >/dev/lp0
terra:~ #  echo -en "\f" >/dev/lp0
```

dovrebbe quindi essere possibile stampare correttamente qualsiasi file di testo ASCII su ogni stampante idonea a stampare un testo ASCII che usa il set di caratteri DOS/Windows.

Se ciò funziona, è consigliabile creare un filtro per la stampante che esegua automaticamente la conversione del file di testo ASCII nel formato specifico della stampante.

Esempio di un filtro della stampante proprio

Innanzitutto, creeremo una sottodirectory per il filtro e vi entriamo come `root`:

```
terra:~ #  mkdir /usr/local/il-mio-filtro-della-stampante
terra:~ #  cd /usr/local/il-mio-filtro-della-stampante
```

Create uno script bash (come file di testo ASCII) con il nome `asciifilter`, proprio illustrato nel file 23.

```
#!/bin/bash

# make a temporary file
INPUT="$(mktemp /tmp/asciifilter.$$.XXXXXX)"

# First store everything from stdin in $INPUT
# to have the input as a regular file
cat >$INPUT

# Recode the INPUT
recode lat1..ibmpc $INPUT

# Add a FormFeed at the end of $INPUT
# to get the last page out of the printer
echo -en "\f" >>$INPUT

# Send $INPUT to stdout
cat $INPUT

# Remove the INPUT file
rm $INPUT
```

file 23: */usr/local/il-mio-filtro-della-stampante/asciifilter*

Rendete questo script eseguibile per ogni utente con

```
terra:~ #  chmod -v a+x /usr/local/il-mio-filtro-della-stampante/
terra:~ #  chmod -v a+rx /usr/local/il-mio-filtro-della-
     stampante/asciifilter
```

Create con `lprsetup` una coda supplementare (vd. `lprsetup --help`). Qui la chiamiamo `af` (ovvero “asciifilter”).

```
terra:~ #  lprsetup -add af -lprng -device /dev/lp0 -raw -sf
```

In `/etc/printcap`, alla voce `af` sostituite solamente nella riga `if` il path `/usr/lib/lpdfilter/bin/if` con `/usr/local/il-mio-filtro-della-stampante/asciifilter`, in modo che alla fine la registrazione `af` abbia il seguente aspetto:

```
af:\
        :cm=lpdfilter drv= method=raw color=no:\
        :lp=/dev/lp0:\
        :sd=/var/spool/lpd/af:\
        :lf=/var/spool/lpd/af/log:\
        :af=/var/spool/lpd/af/acct:\
        :if=/usr/local/il-mio-filtro-della-stampante/asciifilter:\
        :la@:mx#0:\
        :tr=:cl:sh:
```

file 24: */etc/printcap: filtro proprio*

Fermate e riavviate lo spooler di stampa con

```
terra:~ #  rclpd stop
terra:~ #  rclpd start
```

Ora, tutti gli utenti dovrebbero essere in grado di stampare tramite la nuova coda af, con il comando

```
tux@terra:~ >  lpr -Paf file ascii
```

Il sistema di stampa CUPS

Terminologia

Con "client" o "programma client" si indica un programma che viene inizializzato per inviare degli incarichi da stampare al demone CUPS.

Un "demone" è un servizio locale che riceve gli incarichi di stampa e li inoltra o li elaborare.

Un "server" è un demone che fornisce a una o più stampanti 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".

IPP e server

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

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

Con la funzione "broadcast" del demone CUPS, le stampanti locali gestiti dallo stesso demone possono essere rese disponibili nella rete (porta UDP 631) e appaiono come coda sui demoni che ricevono/analizzano, cosa che potete configurare, i pacchetti broadcast. Questo è un vantaggio per reti aziendali, perché permette di "vedere", dopo l'avvio del computer, tutte le stampanti a disposizione, senza dover configurare manualmente alcunché. Questo comunque comporta un rischio quando il computer è collegato ad Internet. Configurando la funzionalità broadcast dovete far sì che il broadcast si propaghi solo all'interno della rete locale, che l'accesso sia permesso solo alla rete locale e che l'indirizzo IP pubblico per la connessione ad Internet non si trovi nell'area degli indirizzi della rete locale, altrimenti anche altri utenti dello stesso ISP potrebbero "vedere" le stampanti condivise rese note dal broadcast e utilizzarle. Inoltre i broadcast generano traffico di rete, cosa che può comportare dei costi aggiuntivi. Per tale ragione bisogna sempre assicurarsi che i pacchetti broadcast non vengano inviati dalla stampante locale su Internet, per esempio con il firewall di SuSE che filtra i pacchetti. Per ricevere degli broadcast non si deve configurare in aggiunta alcunché. Solo all'invio deve venire indicato un indirizzo broadcast (per esempio da configurare tramite YaST).

L'IPP viene utilizzato per la comunizione 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 della 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.

Configurazione del server CUPS

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

Attenzione

L'interfaccia Web comporta il rischio di compromettere la password di root, poiché la password di root viene trasmessa in forma non cifrata, ovvero in chiaro appena 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 appare un messaggio di errore.

Per amministrare stampanti locali è necessario che un demone CUPS giri su un computer locale. A tal fine si deve installare il pacchetto `cups` e i file PPD generati da SuSE in `cups-drivers` e `cups-drivers-stp`. Poi si lancia il server (come `root`) con il comando: `/etc/rc.d/cups restart`. Nel processo di configurazione con YaST l' installazione e l'avvio avvengono implicitamente selezionando CUPS quale sistema di stampa e installando la stampante.

PPD sta per "PostScript Printer Description" ed è uno standard per descrivere le opzioni della stampante con comandi PostScript. A CUPS servono per la procedura di installazione della stampante. SuSE Linux fornisce file PPD per stampanti di diverse case produttrici. Comunque, anche le case prodruttici mettono a disposizione, su Internet e/o CD di installazione, file PPD per stampanti (soprattutto nella sezione "Installazione sotto Windows NT").

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

Il broadcast si configura con YaST, o nel file `/etc/cups/cupsd.conf` si può impostare la variabile "Browsing" su `On` (default) e assegnando alla variabile "BrowseAddress" 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 accettare incarchi

di stampa. Dovete completare `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.

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 collegati ad un cosiddetto print server box o router box con funzionalità di server di stampa o simili. 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 verificarlo servendovi del seguente comando:

```
netcat -z nome-del-computer.dominio 515 && echo ok || echo failed
```

Se questo servizio è disponibile, allora lo si può configurare con il device URI (gergo CUPS), una stringa del tipo `lpd://Server/Queue`. Per ulteriori dettagli a riguardo, vedi `file:/usr/share/doc/packages/cups/sam.html`.

Di solito è preferibile indirizzare queste stampanti tramite la porta 9100 (HP, Kyocera e tanti altri) integrata o la porta 35 (QMS), cioè senza frapporre un protocollo LPD. Il device URI in questo caso è `socket://Server:Port/`.

Per poter stampare con stampanti Windows deve essere installato il pacchetto `samba-client` e Samba deve essere configurato in modo corretto, cioè deve essere impostato il giusto "work group", etc. Esistono diversi tipi di device URI 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 la pagina di manuale di `smbspool` (`man 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.). In tal modo per esempio non sarebbe più necessario cambiare la configurazione, p.e. la dimensione standard dei fogli su `Letter` per ogni singolo client, bastarebbe farlo una volta solo sul server (vd. sezione *Impostazione della coda* a pagina 175). La configurazione viene salvata localmente, ma viene applicata anche agli altri client attraverso i tool CUPS, o meglio grazie al protocollo IPP.

Elaborazione interna dell'incarico

Conversione in PostScript

In linea di massima ogni tipo di file può essere inviato ad un demone CUPS, ma i file PostScript in questo constesto non creano alcun problema di sorta. La conversione in PostScript attraverso CUPS avviene dopo che il tipo di file è stato identificato sulla base di `/etc/cups/mime.types` e di seguito viene lanciato il corrispondente tool che si trova in `/etc/cups/mime.convs`. Il processo di conversione avviene sul server e non sul client. Lo scopo è quello di eseguire la conversione solo sul server preposto alla stampante.

Conteggio delle pagine

Dopo la conversione in PostScript, viene determintato il numero delle 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 in `/var/log/cups/page_log`.

Le registrazioni sono:

- Nome della stampante (p.e. `lp`),
- Nome dell'utente (p.e. `root`),
- Numero dell'incarico,
- Data nella parentesi quadra [],
- Il numero 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 certe 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 dati specifici da stampare. Questi filtri si trovano sotto `/usr/lib/cups/filter/`. Quale filtro è quello indicato, viene stabilito nel file PPD alla voce `*cupsFilter`. Se non vi è alcuna registrazione si presume che si dispone di una stampante PostScript. Tutte le opzioni che dipendono dal dispositivo, come la risoluzione e la dimensione dei fogli, vengono elaborati da questo filtro.

Non è facile e dunque non è consiliabile compilare propri filtri per stampanti.

Invio dei dati alla stampante

Infine viene richiamato il back-end. Si tratta di un filtro speciale che invia 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 dal device URI indicato durante l'installazione). Un back-end può essere per esempio `usb`, in questo caso verrebbe lanciato il programma `/usr/lib/cups/backend/usb`, aperto il dispositivo USB (e bloccato) nel file system, pre-inizializzato ed inoltrati i dati provenienti dal filtro. Alla fine, il dispositivo viene chiuso e rimesso a disposizione del sistema.

Attualmente esistono back-end paralleli, seriali, usb, ipp, lpd, http, socket (nel pacchetto CUPS), ed inoltre canon e epson (da `cups-drivers-stp`), e smb (da `samba-client`).

Stampare 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 vengono inizializzati altri filtri importanti. Nel caso di altri tool di CUPS le opzioni sono simili.

Consigli & Trucchetti

OpenOffice

OpenOffice supporta CUPS, dunque se stampante da OpenOffice non dovete più, come era il caso per StarOffice 5.2, configurare le stampanti singolarmente. OpenOffice "vede" se è in esecuzione un demone C UPS e chiede automaticamente quali sono le stampanti e le opzioni disponibili. In futuro non dovrebbe essere più necessario configurare ulteriormente OpenOffice.

Windows

Le stampanti collegate ad un computer Windows possono essere indirizzate tramite il device URI `smb://server/printer` – vedi sopra.

Nel caso inverso, se si vuole stampare con Windows servendosi di un server CUPS, nel file di configurazione Samba `/etc/samba/smb.conf` deve venir immessa la registrazione `printing = cups` o `printing = CUPS` e riavviare il server smb – vedi anche `file:/usr/share/doc/packages/cups/sam.html`

Stampante raw

Si può configurare una stampante raw ovvero grezza ommettendo il file PPD durante l'installazione, cioè non vi sarà né filtraggio né 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 (per esempio di solito un'altra risoluzione) possono essere modificate e salvate dagli utenti. Le modifiche vengono memorizzate nel file `~/.lpoptions`. Se una stampante "riconfigurata" viene staccata dal server, rimane visibile nei diversi tool, come `kprinter` o `xpp`. Anche se non esiste più, può essere selezionata, cosa che chiaramente comporta dei problemi. Utenti più esperti sapranno cancellare le righe imputate senza difficoltà alcuna da `~/.lpoptions` servendosi di un editor. Si veda a riguardo l'articolo nella nostra banca dati di supporto *Print Settings with CUPS*.

Compatibilità con LPR

CUPS può anche ricevere incarichi da sistemi LPR. Le impostazioni necessarie in `/etc/inetd.conf` possono essere eseguite con YaST, oppure eliminando il simbolo di commento all'inizio della riga "printer" in `/etc/inetd.conf`. Per esempio (come `root`) con:

```
perl -pi -e 's:^\# (printer):$1:' /etc/inetd.conf
rcinetd reload
```

Per tornare di nuovo a LPRng, alla riga va preposto nuovamente il simbolo di commento:

```
perl -pi -e 's:^(printer):# $1:' /etc/inetd.conf
rcinetd reload
```

Il debug con 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 dopo aver immesso `rccups reload` cupsd rileggerà i file di configurazione modificati. In seguito troverete dei messaggi dettagliati in `/var/log/cups/error_log` che vi aiuteranno ad individuare la causa di eventuali difficoltà.

Con

```
terra:~ #  echo LABEL $(date) | tee -a /var/log/cups/error_log
```

si può applicare una label o etichetta prima del test che verrà riportata proprio così in `/var/log/cups/error_log` per poter poi rintracciare più facilmente i messaggi.

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.

Per code di stampa locali

Generare incarichi di stampa

Di solito si stampa nel modo "System V" con

```
tux@terra:~ > lp -d ⟨coda⟩ ⟨file⟩
```

o nel modo "Berkeley" con

```
tux@terra:~ > lpr -P⟨coda⟩ ⟨file⟩
```

Ulteriori informazioni sono reperibili nella pagina di manuale di `lpr` (`man lpr`) e nella pagina di manuale di `lp` (`man 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. Per ulteriori informazioni vedi la pagina di manuale di `lpr` (`man lpr`) e la pagina di manuale di `lp` (`man lp`) nonché la 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 della coda viene indicato per "System V" con

```
tux@terra:~ > lpstat -o ⟨coda⟩ -p ⟨coda⟩
```

o e per "Berkeley" con

```
tux@terra:~ > lpq -P⟨coda⟩
```

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

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

Ulteriori informazioni nella pagina di manuale di `lpq` (`man lpq`), nella pagina di manuale di `lpstat` (`man lpstat`) e 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

Perl "System V"

```
tux@terra:~ >  cancel ⟨coda⟩-⟨numero dell'incarico⟩
```

o per "Berkeley"

```
tux@terra:~ >  lprm -P⟨coda⟩ ⟨numero dell'incarico⟩
```

cancella l'incarico dalla coda indicata che ha il numero dell'incarico indicato.

Ulteriori informazioni nella pagina di manuale di `lprm` (`man lprm`) e nella pagina di manuale di `cancel` (`man cancel`) e nella sezione "Using the Printing System" sotto
`file:/usr/share/doc/packages/cups/sum.html#USING_SYSTEM`
nel *CUPS Software Users Manual*.

Impostazione della coda

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, a prescindere dall'hardware utilizzato, 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 e con il comando

```
tux@terra:~ >  lpoptions -p ⟨coda⟩ -l
```

vengono mostrate nella forma seguente:

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

laddove un * davanti al valore della opzione indica l'impostazione attuale.

Esempio:

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

Nell'esempio l'opzione `PageSize` è impostata su `A4` e la risoluzione sul valore `300`.

Con

```
tux@terra:~ >  lpoptions -p ⟨coda⟩ -o opzione=valore
```

può essere impostato un valore diverso.

Nell'esempio di sopra con

```
tux@terra:~ >  lpoptions -p ⟨coda⟩ -o PageSize=Letter
```

la dimensione del foglio viene impostata su `Letter` per la relativa coda.

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

Se l'utente `root` immette il comando `lpoptions`, le impostazioni vengono salvate nel file `/etc/cups/lpoptions` come impostazione di default per tutti gli utenti del computer locale. Comunque non viene modificato il file PPD.

Solo se si modificano le impostazioni di default nel file PPD di una coda, esse saranno valide per tutti gli utenti nella rete che si servono di questa coda per stampare.

L'amministratore del sistema può modificare le impostazioni di default nel file PPD di una coda con

```
terra:~ #  lpadmin -p ⟨coda⟩ -o opzione=valore
```

così nell'esempio di sopra con

```
terra:~ #  lpadmin -p ⟨coda⟩ -o PageSize=Letter
```

viene impostata la dimensione di default della carta su `Letter` per la corrispondente coda e per tutti gli utenti nella rete.

Vedi anche l'articolo nella banca dati di supporto della SuSE *Print Settings with CUPS*.

Code remote

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

Qui vengono indicati solo i comandi principali. Per quanto riguarda opzioni ulteriori e fonti di informazioni, vedi la sezione *Per code di stampa locali* a pagina 174.

Generare incarichi di stampa

Per " System V " con

```
tux@terra:~ >  lp -d ⟨coda⟩ -h server-di-stampa ⟨file⟩
```

o per "Berkeley" con

```
tux@terra:~ >  lpr -P⟨coda⟩@server-di-stampa ⟨file⟩
```

si genera l'incarico nella coda indicata sul server di stampa indicato.

Premessa: il server di stampa è configurato in modo che si disponga del permesso di stampare servendosi delle sue code. Di default questo non è possibile con CUPS, ma con la configurazione della stampante tramite YaST, in un sottomenu, si ha la possibilità di modificare le impostazione per il server CUPS.

Visualizzare lo stato

Per "System V" con

```
tux@terra:~ >  lpstat -h server di stampa -o ⟨coda⟩ -p ⟨coda⟩
```

viene visualizzato lo stato di una coda sul server di stampa.

Cancellare incarichi di stampa

Il comando per "System V"

```
tux@terra:~ >  cancel -h server di stampa ⟨coda⟩-⟨numero
     dell'incarico⟩
```

cancella l'incarico con il numero d'incarico indicato dalla coda sul server di stampa.

Eliminare disfunzioni in CUPS con il comando di cui sopra

Si procede in modo analogo alla sezione *Eliminare disfunzioni in LPRng con i comandi descritti sopra* a pagina 152, con la sola differenza che con CUPS nella seconda parte si devono immettere altri comandi:

1. Togliete i fogli per terminare il processo di stampa.
2. Con `lpstat -o` (o con `lpstat -h server di stampa -o`) controllate da quale coda si sta stampando e cancellate l'incarico con `cancel` ⟨*coda*⟩-⟨*numero dell'incarico*⟩ (o con `cancel -h server di stampa` ⟨*coda*⟩-⟨*numero dell'incarico*⟩).

3. Utilizzate eventualmente il comando `fuser`.

4. Resettate la stampante.

Su Ghostscript

Ghostscript accetta dati PostScript e PDF. Per la conversione in altri formati, esso contiene una serie di driver, chiamati "device".

Il processo di conversione di Ghostscript è diviso in due fasi:

1. I dati PostScript vengono risolti in una matrice: la grafica descritta 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 necessita un aumento dei punti del reticolo ed comporta una quadruplicazione della memoria richiesta.

2. La grafica scomposta in punti viene ora convertita dal driver scelto nel formato (per esempio linguaggio della stampante) desiderato.

Ghostscript non vi offre solo driver per stampanti. Ghostscript può anche convertire file PostScript in file per l'output sullo schermo o in file PDF.

Per convertire file PostScript in documenti da visualizzare comodamente sullo schermo, usate il programma gv (pacchetto `gv`) che offre un'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 si trova oltre che nella pagina di manuale di `gs` (`man gs`) e nella lista dei driver di Ghostscript anche sotto:

`file:/usr/share/doc/packages/ghostscript/catalog.devices`

e, soprattutto, sotto:

```
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 lanciate Ghostscript direttamente dalla riga di comando, si avvia anche un dialogo con un proprio prompt GS>, che potete chiudere con il comando `quit`.

Il comando di aiuto `gs -h` elenca tutte le opzioni principali e fornisce una lista attuale dei "device" supportati, indicando solo la denominazione generale del driver, come `uniprint` o `stp` (se un solo driver supporta più modelli). I file con i parametri per `uniprint` ed i modelli di `stp` sono elencati, uno per uno, sotto `file:/usr/share/doc/packages/ghostscript/catalog.devices`.

Esempi di impiego di Ghostscript

Sotto `file:/usr/share/doc/packages/ghostscript/examples` troverete dei file esempio PostScript.

La "ellisse cromatica" `file:/usr/share/doc/packages/ghostscript/examples/colorcir.ps` si adatta bene ad un prova di stampa.

Output di X11

Su X, la superficie grafica, potete visualizzare un file PostScript con il comando `gs`:

```
tux@terra:~ >  gs -r60 \
     /usr/share/doc/packages/ghostscript/examples/colorcir.ps
```

Immettete il comando in una sola riga senza (`'\'`).

Con l'opzione `-r`, viene indicata la risoluzione, che dovrà essere adatta al dispositivo in questione (stampante o schermo), provate p.es. con `-r30`. Per chiudere il programma, premete, nella finestra del terminale in cui avete dato il comando `gs`, i tasti Ctrl + c .

Conversione in PCL5e

La conversione di un file PostScript nel formato di una stampante PCL5e o PCL6 si ha, ad esempio, con il comando:

```
tux@terra:~ >  gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn
     \
     -sDEVICE=ljet4 -r300x300 \
     /usr/share/doc/packages/ghostscript/examples/colorcir.ps \
     quit.ps
```

laddove il comando va immesso 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 di una stampante PCL3 si ha, ad esempio, con i comandi

```
tux@terra:~ >  gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn
     \
     -sDEVICE=deskjet -r300x300 \
     /usr/share/doc/packages/ghostscript/examples/colorcir.ps \
     quit.ps

tux@terra:~ >  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

tux@terra:~ >  gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn
     \
     -sDEVICE=cdjmono -r300x300 \
     /usr/share/doc/packages/ghostscript/examples/colorcir.ps \
     quit.ps

tux@terra:~ >  gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn
     \
     -sDEVICE=cdj500 -r300x300 \
     /usr/share/doc/packages/ghostscript/examples/colorcir.ps \
     quit.ps

tux@terra:~ >  gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn
     \
     -sDEVICE=cdj550 -r300x300 \
     /usr/share/doc/packages/ghostscript/examples/colorcir.ps \
     quit.ps
```

(Ogni comando deve rientrare in un'unica riga senza `'\'`.)

Conversione in ESC/P, ESC/P2 o ESC/P raster

La conversione di un file PostScript in un formato di stampante ESC/P2, ESC/P o ESC/P raster si ha, ad esempio, con i comandi:

```
tux@terra:~ >  gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn
     \
     @stcany.upp \
```

```
     /usr/share/doc/packages/ghostscript/examples/colorcir.ps \
     quit.ps

tux@terra:~ >  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 la sintassi del comando nel caso in cui si usa un file parametro `stcany.upp` 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 driverGhostscript, non serve specificarne altri.

Stampare in modo diretto

Dopo che comando di cui sopra sono stati eseguiti, i dati da stampare risiedono in `/tmp/out.prn`, che a questo punto con il seguente comando di `root`, possono essere inviati direttamente alla stampante (dunque ricorrere a spooler o filtro di stampante), se la stampante è collegata alla prima porta parallela `/dev/lp0`:

```
terra:~ #  cat /tmp/out.prn >/dev/lp0
```

L'elaborazione di file 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 da PostScript a PDF:

```
tux@terra:~ >  gs -q -dNOPAUSE -dSAFER
     -sOutputFile=/tmp/colorcir.pdf \
     -sDEVICE=pdfwrite \
     /usr/share/doc/packages/ghostscript/examples/colorcir.ps \
     quit.ps
```

Riconvertire il file PDF `/tmp/colorcir.pdf` appena generato nuovamente in PostScript:

```
tux@terra:~ >  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.

Fondere file PostScript e file PDF in un file PostScript:

```
tux@terra:~ >  gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.ps \
     -sDEVICE=pswrite \
     /usr/share/doc/packages/ghostscript/examples/escher.ps \
     /tmp/colorcir.pdf quit.ps
```

Fondere file PostScript e file PDF in un file PDF:

```
tux@terra:~ >  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 della fusione di file PostScript e file PDF dipende dai file utilizzati.

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 di ricevere un file PostScript. A tal fine utilizzate il programma a2ps (pacchetto `a2ps`).

a2ps è uno strumento potentissimo per generare da semplici file di testo stampe PostScript di ottima qualità.

a2ps è un programma versatile con molte opzioni per la riga di comando. La documentazione principale si trova nella pagina di manuale di `a2ps` (`man a2ps`) – quella completa nella pagina info di `a2ps`.

Esempi di impiego di a2ps

Stampare direttamente 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, potete inserire il seguente comando:

```
tux@terra:~ >  a2ps -2 --medium=A4dj --output=/tmp/out.ps file-
     di-testo
```

Potete visualizzare un'anteprima di stampa di a2ps sulla superficie grafica, con il comando

```
tux@terra:~ >  gs -r60 /tmp/out.ps
```

Nella finestra di terminale in cui avete inserito il comando `gs`, dovrete premere invio per passare alla pagina successiva. Per chiudere, premete Ctrl + c.

Per convertire l'output di a2ps nel formato della stampante, inserite

```
tux@terra:~ >  gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn
     \
     ⟨parametro-del-driver⟩ /tmp/out.ps quit.ps
```

laddove ⟨*parametro-del-driver*⟩ dovrà adattarsi alla stampante. Vd. paragrafo precedente.

Per inviare l'output di Ghostscript, come utente `root`, direttamente alla stampante (senza passare per spooler e filtro), immettete

```
terra:~ #  cat /tmp/out.prn >/dev/lp0
```

a condizione che la stampante sia collegata alla prima porta parallela `/dev/lp0`.

Stampare biglietti da visita

Per darvi un assaggio della versatilità di a2ps, stamperemo ora dei semplici biglietti da visita. Create un biglietto da visita con un semplice file di testo `card`

```
Titolo Nome Cognome
Via
CAP Località
E-mail: utente@dominio
Telefono: prefisso-numero
```

file 25: *card: un biglietto da visita*

Aggiungete il simbolo ASCII\f (formfeed), in modo che a2ps stampi ogni biglietto come se fosse una pagina a se stante.

```
tux@terra:~ >  echo -en "\f" >>card
```

Riproduzione di 10 pezzi in un file `cards`:

```
tux@terra:~ >  for i in $(seq 1 10) ; do cat card >>cards ; done
```

Determinare la riga più lunga su `cards`:

```
tux@terra:~ >  cat cards | wc -L
```

Convertire in PostScript, in modo tale che tutti i 10 biglietti da visita siano distribuiti in due colonne da 5 biglietti su un foglio, con una cornice per ogni biglietto e con un testo non eccedente la riga più lunga, senza intestazione o pié di pagina:

```
tux@terra:~ >  a2ps -i -j --medium=a4dj --columns=2 --rows=5 \
     --no-header --chars-per-line=numero --output=cards.ps cards
```

Il comando deve occupare una sola riga senza (`'\'`) e per `numero` immettete il numero di caratteri della riga più lunga più 1.

Dopo aver controllato tutto allo schermo con `gs -r60 cards.ps`, avviate il processo di stampa in modo diretto come descritto sopra, oppure con il comando `lpr` ricorrendo al relativo sistema di stampa con `lpr cards.ps`.

Convertire in 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 si tratti effettivamente di 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 di `pstops` (`man 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 la conversione, cosa che di solito è possibile, ma a seconda degli applicativi con cui è stato creato il file PostScript, ciò non potrebbe essere possibile.

psnup

Con

```
tux@terra:~ >  psnup -2 /tmp/in.ps /tmp/out.ps
```

`/tmp/in.ps` diventa `/tmp/out.ps` con due pagine ridimensionate l'una accanto all'altra su di 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.

pstops

Questo comando consente di impostare la dimensione e posizione del testo nel modo desiderato:

```
tux@terra:~ >  pstops '1:0@0.8(2cm,3cm)' /tmp/in.ps /tmp/out.ps
```

Con il fattore 0.8 una pagina A4 di ca. 21x30 cm viene scalata (ridotta) a ca. 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 tanto ed inoltre si avranno margini generosi, dunque si adatta particolarmente a quei applicativi che vogliono far rientrare tanto in una pagina - come per esempio `/tmp/in.ps`, dove non tutto il testo sarebbe rientrato in un foglio.

Con

```
tux@terra:~ >  pstops '1:0@0.8(2cm,3cm)' /tmp/in.ps /tmp/out1.ps
tux@terra:~ >  psnup -2 /tmp/out1.ps /tmp/out.ps
```

si hanno due pagine notevolmente ridotte, l'una accanto all'altra su un foglio – però con tanto spazio tra le due pagine ridotte.

Si raggiungono miglior risultati se si posizionano le pagine singolarmente:

```
tux@terra:~ >  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 conteggiate in modo alternato una volta come pagina 0 (modulo 2) e una volta come pagina 1 (modulo 2).

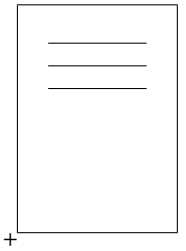
0L@0.6(20cm,2cm) significa, che la pagina 0 (modulo 2) viene girata per 90 gradi verso sinistra, scalata del fattore 0.6, e in seguito spostata di 20cm verso destra e di 2cm in alto.

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.

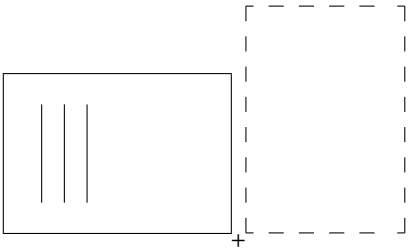
Illustrazione:

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 +.

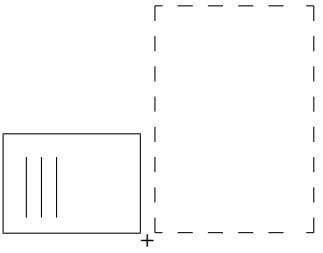
Ecco una pagina 0 (modulo 2) con tre righe di testo:



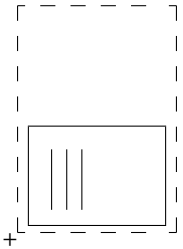
Dopo una rotazione verso sinistra di 90 gradi:



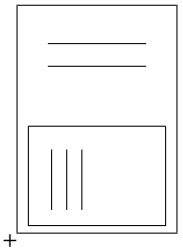
Dopo essere stata scalata del fattore di 0.6:



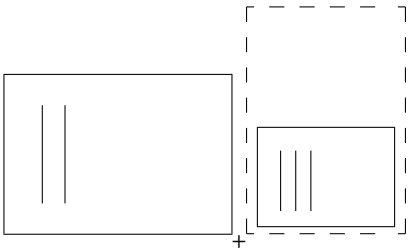
Dopo essere stata spostata di 20cm verso destra e di 2cm verso l'alto:



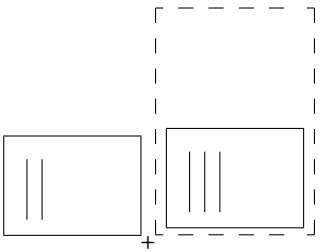
Sovrapposizione della pagina 1 (modulo 2) con due righe di testo:



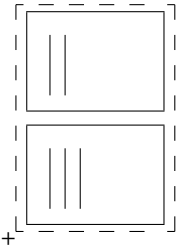
Dopo una rotazione verso sinistra della pagina 1 (modulo 2) di 90 gradi:



Dopo aver scalato la pagina 1 (modulo 2) del fattore 0.6:



Dopo aver spostato la pagina 1 (modulo 2) di 20 cm verso destra e di 15 cm verso l'alto:



psselect

Con psselect potete selezionare singole pagine.

Con

```
tux@terra:~ >  psselect -p2-5 /tmp/in.ps /tmp/out.ps
```

selezionate da /tmp/in.ps le pagine 2,3,4 e 5 e le spostate in /tmp/out.ps.

Con

```
tux@terra:~ >  psselect -p-3- /tmp/in.ps /tmp/out.ps
```

selezionate tutte le pagine fino alla pagina 3.

Con

```
tux@terra:~ >  psselect -r -p4- /tmp/in.ps /tmp/out.ps
```

vengono selezionate tutte le pagine a partire da pagina 4 fino all'ultima ed emesse in ordine inverso.

Verifica allo schermo con Ghostscript

Immettendo `gs -r60 /tmp/out.ps` il file PostScript `/tmp/out.ps` può essere visualizzato pagina per pagina tramite l'interfaccia grafica di Ghostscript. Premete il tasto invio nella finestra di terminale nella quale avete richiamato Ghostscript, per scorrere le singole. Per uscire, premete Ctrl + c.

Il programma `gv` nel pacchetto `gv` è un front-end grafico per Ghostscript. Si lancia con `gv /tmp/out.ps` e consente soprattutto una buona rappresentazione del formato orizzontale, dell'ingrandimento o del ridimensionamento (però non nel file PostScript in sé) e di selezionare singole pagine - soprattutto anche per stampare direttamente da `gv`.

La codificazione di testi ASCII

Nel caso di semplici file di testo ogni carattere è rappresentato da una combinazione di numeri. In una apposita tabella è riportato quale codice numerico corrisponde a quale carattere. A seconda della tabella di codifica di un determinato programma o filtro della stampante, 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 "soliti", non inclusi sono i caratteri speciali di una determinata lingua), che sono sempre identici per ogni lingua.

I codici 128 fino a 255 sono riservati ai caratteri speciali di ogni lingua (per esempio gli umlaut tedeschi).

Dato che vi sono molto più che 128 caratteri speciali se consideriamo tutte le lingue, i codici da 128 fino a 255 non sono dappertutto uguali, ma a secondo della locazione geografica lo stesso codice viene utilizzato per i diversi caratteri speciali 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 la codificazione delle lingue dell'Europa centro-orientale. Quindi per esempio 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 164).

Illustrazione

Tutti i comandi dovranno rientrare in una sola riga, senza (`'\'`) a *fine riga*.

Generare un file esempio di testo ASCII con

```
tux@terra:~ >  echo -en "\rCode 241(octal): \
     \241\r\nCode 244(octal): \244\r\f" >example
```

Visualizzazione allo schermo

Aprire tre finestre di terminale nell'interfaccia grafica con

```
tux@terra:~ >  xterm -fn -*-*-*-*-*-*-14-*-*-*-*-*-iso8859-1 \
     -title iso8859-1 &
```

```
tux@terra:~ >  xterm -fn -*-*-*-*-*-*-14-*-*-*-*-*-iso8859-15 \
     -title iso8859-15 &
tux@terra:~ >  xterm -fn -*-*-*-*-*-*-14-*-*-*-*-*-iso8859-2 \
     -title iso8859-2 &
```

In ogni finestra di terminale, potete visualizzare il file d'esempio con i comandi

```
tux@terra:~ >  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 per esempio il simbolo del'euro non può essere utilizzato assieme alla A con l'ogonek nello stesso testo.

Per ulteriori approfondimenti sulla codificazione giusta, consultate:

Per "iso8859-1" la pagina di manuale di `iso_8859-1` (`man iso_8859-1`).

Per "iso8859-15" la pagina di manuale di `iso_8859-15` (`man iso_8859-15`).

Per "iso8859-2" la pagina di manuale di `iso_8859-2` (`man iso_8859-2`).

Stampare

A seconda della codificazione impostata per una coda, i testi ASCII (per esempio il 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 ottiene un foglio con la codificazione utilizzata dal sistema di stampa per il testo ASCII.

Con `a2ps` è possibile convertire il file `example` in PostScript, e stabilire il sistema di codificazione:

```
tux@terra:~ >  a2ps -1 -X ISO-8859-1 \
     -o example-ISO-8859-1.ps example
```

```
tux@terra:~ >  a2ps -1 -X ISO-8859-15 \
     -o example-ISO-8859-15.ps example
tux@terra:~ >  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`.

Stampare nella rete TCP/IP

Per informazioni utili sullo spooler della stampante LPRng consultate l'*LPRng-Howto* sotto
`file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html`

Per CUPS vedi *CUPS Software Administrators Manual* sotto
`file:/usr/share/doc/packages/cups/sam.html`

Terminologia

Server di stampa Di seguito chiameremo "server di stampa" un computer completo con sufficiente potenza di calcolo e capacità di memoria.

Print server box o stampante di rete

- Un "print server box" è un piccolo dispositivo con una connessione di rete TCP/IP da una parte ed la possibilità di connessione locale per una stampante dall'altra. Vi sono anche "box di router" che dispongono di una possibilità di connessione per una stampante e che vanno trattati come print server 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 print server box integrato. Stampanti di rete e print server box vanno dunque gestiti nello stesso modo.

Sussiste una grande differenza tra una stampante di rete o print server box da una parte e un server di stampa vero e proprio dall'altra. Vi sono anche grosse stampanti corredati da un server di stampa per poter stampare via rete. Ma in questo caso per stampare, viene indirizzato il server di stampa fornito a corredo, e non la stampante.

ServerLPD Un "server LPD" è un server di stampa indirizzabile tramite il protocollo LPD, per esempio nel caso in cui sul server di stampa giri il sistema di stampa LPRng/lpdfilter (o più precisamente l' lpd) o il sistema di stampa CUPS configurato in modo che il computer può essere indirizzato anche tramite il protocollo LPD.

Server IPP o server CUPS Nel caso di "server IPP" oppure "server CUPS" si tratta di server di stampa indirizzabili tramite il protocollo IPP. Ciò è il caso quando sul server di stampa è in esecuzione il sistema di stampa CUPS (o più precisamente cupsd).

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

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 avete 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.

Configurare 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 remote con il comando lpr. Vedi a riguardo la sezione *Tool della riga di comando per LPRng* a pagina 148.

La premessa è che il server LPD sia stato configurato in modo che al client sia consentito di servirsi delle code di stampa sul server di stampa.

Per stampare da applicativi si immette nell'applicativo il comando:

```
tux@terra:~ >  lpr -P⟨coda⟩@⟨server di stampa⟩
```

dunque come nella sottosezione *Gestire code remote* a pagina 151 solo senza l'indicazione di un file.

Alcuni applicativi sono preimpostati per CUPS e devono perciò essere impostati per 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 per stampare riportato sopra.

Questo metodo tramite comando per stampare e 'Stampa tramite programma esterno' non è limitato ad LPRng, ma funziona anche per CUPS. Per CUPS si deve immettere come comando di stampa:

```
tux@terra:~ >  lp -d ⟨coda⟩ -h ⟨server di stampa⟩
```

come descritto nella sezione *Tool della riga di comando per il sistema di stampa CUPS* a pagina 173, solo senza l'indicazione di un file.

Configurare un server di rete CUPS

Se il server di stampa è un server di rete CUPS, allora se configurate la stampante tramite YaST potrete scegliere tra le seguenti possibilità:

CUPS come server (default nella installazione standard) Se non è collegata alcuna stampante in locale, non è stata neanche configurata alcuna coda con YaST. In questo caso cupsd non viene lanciato automaticamente. Per lanciare cupsd bisogna attivare il servizio 'cups' (di solito per il 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 in modo che dopo un breve periodo di attesa sul client sono disponibili le code 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 indrizzo broadcast adatto al client e che il client abbia il permesso di servirsi delle code del server di rete CUPS per stampare.

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

In questo casto sul client non gira alcun cupsd e dunque non vi è neanche nessun file /etc/printcap. Gli applicativi che non possono venire impostati in modo da utilizzare CUPS offrono però solo code 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 del server di rete CUPS.

Protocolli per stampare nella 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 YaST si distingue in base al protocollo e non in base all'hardware.

Stampare tramite il protocollo LPD

L'incarico di stampa viene inviato tramite il protocollo LPD a una coda remota. Chiaramente il sistema emittente che quello destinatario devono supportare il protocollo LPD.

Emittente

LPRng

LPRng supporta il protocollo LPD tramite lpd. Serve una coda locale tramite la quale l'lpd locale possa inoltrare l'incarico di stampa, tramite il protocollo LPD, ad una coda remota.
Nel caso di LPRng ciò funziona anche senza lpd locale. Il programma `lpr` dal pacchetto `lprng` inoltra l'incarico di stampa tramite il protocollo LPD direttamente alla coda remota.

CUPS

CUPS supporta il protocollo LPD esclusivamente tramite il demone CUPS cupsd. Serve una coda locale tramite la quale il cupsd locale possa inoltrare l'incarico di stampa, tramite il protocollo LPD, alla coda remota.

Destinatario

Server di stampa

La stampante è collegata localmente ad un server di stampante ed il server di stampa è indirizzabile tramite il protocollo LPD.

Stampante di rete o print server box

La stampante di rete o il print server box devono essere indirizzabili tramite il protocollo LPD, cosa che di solito è così.

Stampare tramite il protocollo IPP

L'incarico di stampa viene inviato ad una coda remota tramite il protocollo IPP. Sia il sistema emittente che quello destinatario devono supportare il protocollo IPP.

Emittente

LPRng

Attualmente LPRng non supporta il protocollo IPP.

CUPS

CUPS supporta il protocollo IPP tramite il cupsd. Serve una coda locale tramite la quale l'lpd locale possa inoltrare l'incarico di stampa, tramite il protocollo IPP, alla coda remota.
Nel caso di CUPS questo funziona anche senza cupsd locale.
Il programma `lp` dal pacchetto cups-client, xpp o il programma KDE `kprinter` possono inoltrare l'incarico di stampa direttamente alla coda remota tramite il protocollo IPP.

Destinatario

Server di stampa

La stampante è collegata ad un server di stampa locale e il server di stampa è indirizzabile tramite il protocollo IPP.

Stampante di rete o print server box

La stampante di rete o il print server box devono essere indirizzabili tramite il protocollo LPD, cosa che è possibile solo con alcuni dei dispositivi recenti.

Stampare direttamente tramite il socket TCP

In questo caso l'incarico di stampa non viene inviato ad una coda remota, poiché non vi è alcun protocollo (né LPD né IPP), che riesca a gestire incarichi di stampa o code. Invece i dati specifici per la stampante vengono inviati tramite il socket TCP ad una porta TCP remota, cosa che deve essere supportata sia da sistema emittente che da quello destinatario.

Emittente

LPRng/lpdfilter

LPRng supporta il processo di stampa direttamente servendosi del socket TCP via l'lpd. Serve una coda locale attraverso la quale l'lpd locale possa inviare l'incarico di stampa, con i dati specifici della stampante convertiti grazie all'lpdfilter, alla porta TCP remota tramite il socket TCP.
Nel caso di LPRng questo si può fare anche senza lpd locale.
L'opzione `-Y` del programma `lpr` del pacchetto `lprng` invia i dati dell'incarico di stampa via socket TCP direttamente alla porta TCP remota. Vedi la pagina di manuale di `lpr` (`man lpr`).
Comunque questo avviene senza filtro di stampante frapposto, così l'incarico di stampa deve già contenere i dati specifici per la stampante.

CUPS

CUPS supporta il processo di stampa direttamente tramite il socket TCP solo attraverso il cupsd. Serve una coda locale

tramite la quale il cupsd locale possa convertire l'incarico di stampa in dati specifici per la stampante, e poi inviarli via socket TCP alla porta remota TCP.

Destinatario

Stampante di rete o il print server box

La stampante di rete o print server box di solito dispongono di una porta TCP attraverso la quale possono essere inviati direttamente alla stampante i dati da stampare.
Nel caso della stampante di rete HP o print server box JetDirectbox della HP, si tratta di solito della porta 9100 o nel caso di print server box JetDirect con due o tre connessioni per stampanti locali si hanno le porte 9100, 9101 e 9102. Queste porte vengono usate anche da tanti altri print server box. Consultate il manuale del print server box e chiedete in caso di dubbio alla casa produttrice del print server box/stampante di rete, attraverso quale porta la stampante possa essere indirizzata direttamente. Informazioni a riguardo nell' *LPRng-Howto* sotto `file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html`
e lì in particolare sotto
`file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#SECNETWORK`
`file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#SOCKETAPI`
`file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#AEN4858`

Stampare tramite il protocollo SMB

L'incarico di stampa, che deve già contenere i dati specifici per la stampante, viene inviato tramite il protocollo SMB ad una "share" remota allocata ad una stampante remota. Il sistema emittente e quello destinatario devono supportare il protocollo SMB. Né LPRng né CUPS supportano direttamente il protocollo SMB. Il sistema di stampa LPRng/lpdfilter usa però smbclient e CUPS usa smbspool (entrambi dal pacchetto `samba-client`). Così entrambi i sistemi di stampa supportano, seppure indirettamente, il protocollo SMB.

Emittente

LPRng/lpdfilter

LPRng supporta il protocollo SMB tramite l'lpdfilter. E' necessaria una coda locale tramite la quale l'lpd locale possa convertire l'incarico di stampa col lpdfilter in dati specifici per la stampante, in seguito l'lpdfilter invia questi dati servendosi del smbclient, tramite il protocollo SMB, alla share remota.

CUPS

E' necessaria una coda locale tramite la quale il cupsd locale possa convertire l'incarico di stampa in dati specifici per la stampante, per poi inviarli con smbspool tramite il protocollo SMB alla share remota.

Destinatario

Il server di stampa SMB

La stampante è connessa ad un server di stampa SMB. Un server di stampa SMB è normalmente un computer DOS/Windows. Può comunque rivestire questo ruolo anche un server Samba Linux.

Il server di stampa SMB è indirizzabile tramite il protocollo SMB. L'accesso alla stampante (cioè l'accesso alla share corrispondente alla stampante) è attivato in quella sede.

Filtraggio per stampanti di rete

Vi sono le diverse possibilità descritte di seguito in tema di filtraggio per stampanti di rete. E' a questo punto che il file di partenza deve essere convertito nel formato che la stampante riesce ad elaborare – ovvero in formato che la stampante "comprende" (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. Se per stampanti non-PostScript i dati da stampare vengono generati con Ghostscript, allora serve tanta potenza di calcolo soprattutto per stampe cromatiche ad alta risoluzione o fotostampe.

Le stampanti di rete e print server box di solito non hanno un filtro della stampante integrato, perciò è necessario un server di stampa.

Quando si impiega una stampante PostScript, si può anche rinunciare ad un server di stampa. Le stampanti PostScript spesso riescono automaticamente a distinguere tra testo ASCII e PostScript, e riescono a stampare entrambi i formati. Per quanto riguarda caratteri speciali di una particolare lingua in testo ASCII, nella stampante va impostata l'adeguata codificazione dei set di caratteri. Il testo ASCII deve prima essere convertito in PostScript tramite `a2ps` con la codificazione adatta di set di caratteri, o visto che gli applicativi di solito stampano solo testo ASCII o PostScript, in questi casi, se si stampa solo saltuariamente, non è strettamente necessario disporre di un server di stampa.

Le stampanti di rete ed i print server box spesso, se c'è molto da stampare, risultano sovraccariche, in questi casi è necessario un server di stampa con sufficiente capacità di memoria per consentire che gli incarichi vengono memorizzati temporaneamente.

Premesse

La stampante deve essere supportata da SuSE Linux, dato che il filtro genera i dati specifici per la stampante come per una stampante collegata localmente; vd. a riguardo la sezione *Configurazione manuale delle porte di una stampante locale* a pagina 139 ss.

Terminologia

- Il "client" è il computer sul quale viene generato l'incarico di stampa.
- "Print server box" indica sia la stampante di rete che il print server box, visto che vanno gestiti nella stessa maniera.
- Con "server di stampa" qui è inteso un solo computer centrale cui tutti i client inviano i loro incarichi. Il server di stampa inoltra i dati alle sue stampanti collegate in locale o tramite rete TCP/IP ai print server box.
- "Forward" indica una coda che non filtra gli incarichi di stampa, ma che li inoltra solo a coda remote.
- "Filtro" indica in generale una coda che filtra incarichi di stampa.
- "Prefiltro" indica una coda che filtra incarichi di stampa e che inoltra il risultato ad una coda Forward sullo stesso computer.
- "Filtro+Forward" indica una coda filtrante incarichi di stampa che inoltra il risultato ad una coda remota.
- "Filtro+Porta" indica una coda filtrante incarichi di stampa che inoltra il risultato ad una porta TCP remota.
- Eventualmente queste denominazioni sono accompagnate da "LPD", "IPP" e "SMB" per indicare il protocollo utilzzato.

Possibilità di filtraggio nel processo di stampa nella rete

Print server box con filtraggio sul client

Dato che il processo del filtraggio avviene sul client, su di esso deve essere in esecuzione un sistema di stampa completo – dunque o il sistema di stampa LPRng/lpdfilter o il sistema di stampa CUPS.

Client utilizza il protocollo LPD (LPRng e CUPS)

Prima prefiltro e dopo forward (solo LPRng)

Il metodo classico consiste di due code sul client: una coda per il filtraggio e una per l'inoltro.

1. Client: convertire l'incarico di stampa in dati da stampare (prefiltro) e trasmetterli alla coda forward come nuovo incarico di stampa.
2. Client: la coda forward inoltra i dati da stampare al print server box (si tratta del cosiddetto LPD forward)
3. Print server box LPD: inviare alla stampante i dati da stampare

Filtro+Forward (LPRng e CUPS) Qui avviene il filtraggio e l'inoltro ad una coda. Per LPRng questo viene indicato con "lpr-bounce" o "lpd-bounce".

1. Client: convertire l'incarico in dati da stampare e inoltrare al print server box (Filtro+ Forward LPD)
2. Print server box LPD: inviare i dati da stampare alla stampante

Client utilizza il protocollo IPP (solo CUPS)

Filtro+Forward (solo CUPS)

1. Client: convertire l'incarico in dati da stampare ed inviarli al print server box (Filtro+Forward IPP)
2. Print server box IPP: inviare i dati da stampare alla stampante

Client utilzza socket TCP (LPRng e CUPS)

Filtro+Porta (LPRng e CUPS)

1. Client: convertire l'incarico in dati da stampare e inviarli al print server box (Filtro+Porta)
2. Print server box: inviare dati da stampare alla stampante.

Print server box con filtraggio sul server di stampa

Dato che il filtraggio avviene sul server di stampa deve girarci un sistema di stampa completo con demone – dunque o il sistema di stampa LPRng/lpdfilter o il sistema di stampa CUPS.

Dato che il filtraggio avviene sul server di stampa, sul client non deve per forza girare un sistema di stampa completo, se sul client gli incarichi di stampa possono essere inviati direttamente al server di stampa tramite il comando `lpr` (per LPRng) o i comandi `lp` o `xpp` o `kprinter` (per CUPS). In questo caso, la premessa ü che il server di stampa supporti il protocollo utilizzato dal client (LPD o IPP).

Dopo che il server di stampa riceve un incarico da stampare, lo elabora come descritto nella sezione *Print server box con filtraggio sul client* per il client.

Il client può inviare al server di stampa l'incarico da stampare tramite un protocollo diverso da quello usato dal server di stampa per inviare i dati da stampare al print server box.

Client usa il protocollo LPD (solo LPRng)

Direttamente (solo LPRng)

1. Client: inviare incarico da stampare al server di stampa (comando `lpr`)
2. Server di stampa LPD: convertire l'incarico da stampare in dati da stampare ed inviare i dati al print server box.

Forward (solo LPRng)

1. Client: inviare incarico da stampare al server di stampa (Forward LPD)
2. Server di stampa LPD: convertire l'incarico da stampare in dati da stampare ed inviarli al print server box.

Client usa il protocollo IPP (solo CUPS)

Direttamente (solo CUPS)

1. Client: inviare l'incarico da stampare al server di stampa (comando `lp` o `xpp` o `kprinter`)
2. Server di stampa IPP: convertire l'incarico da stampare in dati da stampare ed inviarli al print server box.

Stampante collegata al server di stampa e filtraggio sul server di st.

Se la stampante è collegata direttamente al server di stampa, si ha la stessa situazione descritta in *print server box con filtraggio sul server di stampa* (vd. 198), con la sola differenza che, al posto di "inviare i dati della stampante al print server box", si avrà "inviare i dati della stampante alla stampante".

Stampante collegata ad un server di stampa con filtraggio sul client

Per server di stampa LPD ed IPP di solito ciò non conviene. Su ogni client dovrebbe esserci un completo sistema di stampa configurato e funzionante, mentre dovrebbe bastare una configurazione del tipo descritta nella sezione *Stampante collegata a server di stampa e filtraggio sul server di stampa*.

Server di stampa SMB con filtraggio sul client

Sul server di stampa SMB non è previsto alcun filtraggio. Sotto questo aspetto il server di stampa SMB è simile al print server box.

Client usa il protocollo SMB (LPRng e CUPS)

Filtro+SMB-Forward (LPRng e CUPS)

1. Client: convertire incarico di stampa in dati per la stampante ed inviarli al server di stampa SMB (Filtro+SMB-Forward)
2. Server di stampa SMB: inviare dati da stampare alla stampante.

Risolvere dei problemi

Rete TCP/IP

La rete TCP/IP e la risoluzione dei nomi devono funzionare (vedi *Fondamenti del collegamento in rete* a pagina 313).

Controllare la configurazione del filtro

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

Testare un lpd remoto

Con

```
terra:~ #  netcat -z host 515 && echo ok || echo failed
```

potete verificare se l' `host` permette un collegamento TCP all' lpd (porta 515). In caso negativo, il problema è dovuto o all' lpd o alla rete.

Come utente `root` con

```
terra:~ #  echo -e "\004queue" | netcat -w 2 -p 722 host 515
```

si ottiene un resoconto (a volte molto dettagliato) sulle `coda` che si trovano sull' `host` remoto, sempre che l'lpd del computer remoto funzioni ed è possibile inviarci delle richieste. 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 cui tramite `coda` dell' `host` non sia possibile stampare – esempi:

```
lpd: your host does not have line printer access
lpd: queue does not exist
printer: spooling disabled
printer: printing disabled
```

output 12: *Messaggio di errore di lpd*

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

Testare il cupsd remoto

Con

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

verificate se nella rete vi è un server di rete CUPS il quale dovrebbe inviare un broadcast indicando le proprie code ogni 30 secondi. Dopo 40 secondi dovrebbe apparire un output simile a questo, se vi è un server di rete CUPS che invia broadcast:

```
... ipp://Nome-server.dominio:631/stampanti/coda
```

output 13: *Broadcast da un server di rete CUPS*

Con

```
terra:~ #  netcat -z host 631 && echo ok || echo failed
```

verificate se è possibile un collegarsi al cupsd (porta 631) dell'`host` tramite TCP. In caso negativo, il problema è dovuto o al cupsd o alla rete.

Con

```
terra:~ #  lpstat -h host -l -t
```

si ottiene un resoconto (a volte molto dettagliato) sulle `code` che si trovano sull' `host` remoto, sempre che il cupsd del computer remoto funzioni ed è possibile inviarci delle richieste.

Con

```
terra:~ #  echo -en "\r" | lp -d coda -h host
```

verificate se le `code` sull' `host` accettino 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 – dunque avere alla fine solo un foglio bianco.

Testare un server SMB remoto

La funzione principale si lascia testare con:

```
terra:~ #  echo -en "\r" \
     | smbclient '//HOST/SHARE' 'PASSWORD' \
     -c 'print -' -N -U 'USER' \
     && echo ok || echo failed
```

su una sola riga senza backslash `'\'`. Al posto di HOST inserite il nome host del server Samba, per SHARE il nome della coda remota (cioè il nome della share Samba), per PASSWORD la vostra password e per USER il nome dell'utente. Con questo comando si esegue solo un test, normalmente non dovrebbe venir stampato alcunché – e se sì, allora solo un foglio bianco.

Con

```
terra:~ #  smbclient -N -L host
```

visualizzate le share disponibili su `host` – vd. la pagina di manuale di `smbclient` (`man smbclient`).

La stampante di rete o il print server box non funzionano ineccepibilmente

Di solito si verificano dei problemi con lo spooler di stampa del print server box, non appena c'è tanto da stampare. Visto che il problema è dovuto al print server box, non può essere risolto.

Si può aggirare lo spooler indirizzando direttamente la stampante collegata al print server box tramite il socket TCP.

In questo modo il print server 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 print server 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 del print server box.

Comunque in questo caso deve essere nota la relativa porta TCP sul print server box.

Se la stampante è collegata al print server box ed è accesa, tramite il programma `nmap` dal pacchetto `nmap`, dopo aver acceso anche il box, si lascia determinare in poco tempo la porta TCP in questione.

`nmap` emetterà nel caso di un print server box:

```
Port       State       Service
23/tcp     open        telnet
80/tcp     open        http
515/tcp    open        printer
```

```
631/tcp    open        cups
9100/tcp   open        jetdirect
```

- Tramite `telnet` potete entrare nel print server box, in modo da poter ricercare informazioni basilari ed intervenire sulla configurazione.
- Tramite HTTP potete indirizzare un server web che gira su un print server box. Esso fornisce informazioni dettagliate e permette di configurare in modo dettagliato.
- Attraverso la porta 515 potete indirizzare tramite il protocollo LPD lo spooler che gira sul print server box.
- Attraverso la porta 631 potete indirizzare tramite il protocollo IPP lo spooler che gira sul print server box.
- Attraverso la porta 9100 potete indirizzare tramite socket il TCP la stampante collegata al print server box.

Server di stampa LPD ed IPP

Solo con CUPS

Un server CUPS supporta solitamente solo il protocollo IPP. Il programma `/usr/lib/cups/daemon/cups-lpd` del 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'`inetd` con YaST o manualmente, attivando il rigo corrispondente nel file `/etc/inetd.conf`.

LPRng/lpdfilter e CUPS

Alcuni vorranno far girare entrambi i sistema di stampa LPRng/lpdfilter e CUPS sullo stesso computer – forse per aggiungere CUPS al server di stampa LPD, o perché in alcuni casi particolari necessitano 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.

Esistono diverse possibilità. Saremo lieti di fornirvi assistenza nel quadro del nostro servizio SuSE, per i particolari visitate

http://www.suse.de/it/services/index.html
.

- La configurazione della stampante non dovrebbe essere eseguita con YaST, poiché la configurazione della stampante con YaST non è adatta a questi casi.
- Vi è un conflitto tra i pacchetti lprng e cups-client, dato che contengono file omonimi per esempio `/usr/bin/lpr` e `/usr/bin/lp`. Quindi non va installato il pacchetto cups-client che a sua volta comporta la mancanza di tool della riga di comando per CUPS (ve ne sono solo per LPRng). Comunque sarà possibile stampare servendosi delle code CUPS tramite l'interfaccia grafica di xpp o kprinter, e dagli applicativi che supportano direttamente CUPS.
- Per motivi di compatibilità, all'avvio cupsd crea un nuovo file `/etc/printcap` con solo i nomi delle code CUPS, poiché numerosi applicativi leggono i nomi delle code 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 in `/etc/printcap`, mostrano solo queste code locali, e non tutte le code CUPS disponibili sulla rete.

Hotplug

Oggigiorno esistono tante componenti di hardware che possono essere connesse e disconnesse mentre il sistema è in esecuzione. Oltre a USB, quale esempio noto per questo tipo di componente, vi sono inoltre PCI, PCMCIA, Firewire, SCSI e altre interfacce.

I sistemi hotplug hanno il compito di rilevare hardware che è stato appena connesso o integrato e di configurarlo automaticamente in modo che possa essere utilizzato immediatamente dal sistema. Inoltre le componenti che verranno tolte, devono essere preparate a questo intervento e le risorse devono essere rimesse a disposizione se le componenti sono state rimosse senza preavviso.

Hotplug sotto Linux

Di solito i cosiddetti demoni controllano gli eventi esterni dei componenti del sistema. Per esempio inetd controlla le richieste di rete in entrata. Nel caso dell'hotplug è lo stesso kernel che funge da demone. Per realizzare ciò, i driver del bus devono essere in grado di rilevare nuovi componenti e di comunicarli al sistema. Nel kernel 2.4 sono in grado di farlo: USB, PCMCIA, Firewire, in parte PCI e il sottosistema di rete. Questa parte dell'hotplug è parte integrante dei moduli e per apportare delle modifiche bisogna intervenire sul kernel.

Nota

Dispositivi PCMCIA sono atti all'hotplug solo se si tratta di schede CardBus ed è stato selezionato il kernel sistema PCMCIA. Appariranno come dispositivi PCI. Per ulteriori dettagli vedi la sezione che tratta PCMCIA.

Nota

La seconda parte del hotplug prepara l'integrazione dei dispositivi o la loro rimozione. Si tratta di un insieme di script nella directory `/etc/hotplug` con `/sbin/hotplug` quale script principale. Questo script è un'interfaccia tra kernel e l'insieme di script hotplug.
In questo capitolo chiameremo questi script con "sistema hotplug".

Quando si integra o si rimuove un dispositivo hotplug, il kernel richiama lo script `/sbin/hotplug` e gli consegna ulteriori informazioni riguardanti le relative componenti hardware. Questo script distribuisce gli incarichi – a seconda dell'hardware – ad altri script. Questi caricano o scaricano moduli del kernel e richiamano a loro volta ulteriori programmi per la configurazione dei componenti. I programmi risiedono in `/etc/hotplug` e hanno sempre la desinenza `.agent`.

Avvio hotplug e coldplug

Nonostante il kernel trasmetti gli eventi hotplug a `/sbin/hotplug`, il sistema hotplug dovrà essere innanzitutto avviato. Finché l'hotplug non è stato inizializzato, tutti gli eventi vengono scartati.

Inoltre vi sono delle componenti che vengono rilevati dal kernel prima ancora che sia possibile accedere al file system. Gli eventi vanno persi e per questo gli script `/etc/hotplug/*.rc` tentano di generare artificialmente degli eventi per hardware esistente. In questi casi si parla anche di "coldplug".

Se a questo punto non avete ancora caricati i moduli di base USB, essi verranno caricati e il filesystem dei dispositivi USB (`usbdevfs`) verrà annesso.

Se fermate l'hotplug con `rchotplug stop`, anche gli eventi non verranno più analizzati. Chi non modifica le componenti di hardware mentre il sistema è in esecuzione, può anche disabilitare completamente l'hotplug. Comunque va provveduto in un altro modo alla configurazione dei dispositivi USB o PCMCIA.

Nella directory `/etc/sysconfig/hotplug` vi sono delle variabili che controllano il comportamento dell'hotplug. Per esempio con la variabile HOTPLUG_DEBUG potete impostare la cosiddetta "verbosità" di hotplug. Con le variabili ⟨*HOTPLUG_START_USB*⟩, ⟨*HOTPLUG_START_PCI*⟩ e ⟨*HOTPLUG_START_NET*⟩ potete impostare che vengano elaborati solo determinati eventi. Tutte le altre variabili vengono spiegate nei relativi paragrafi.

Tutti i messaggi hotplug vengono protocollati sempre nel file (`/var/log/messages`) (systemlog).

USB

Quando si connette un nuovo dispositivo USB, lo script `/etc/hotplug/usb.agent` determina un driver adatto e assicura che venga caricato. Questo driver non deve essere per forza un modulo del kernel, per esempio tante camere USB vengono indirizzate direttamente dagli applicativi.

L'assegnazione del driver all'hardware è un processo a più gradi: come primo si va a vedere nel file `/etc/hotplug/usb.usermap` se questa componente hardware deve essere gestita da un applicativo o un da uno script di inizializzazione speciale. Altrimenti, in `/etc/hotplug/usb.handmap` si cercherà di assegnarlo individualmente a un modulo del kernel in `/etc/hotplug/usb.handmap`. Se non trovate niente neanche qui (cosa che si verifica il più delle volte), viene interrogata la tabella di assegnazione del kernel `/lib/modules/`⟨*versione_del_kernel*⟩`/modules.usbmap`. Inoltre viene riscandito l'hardware USB che farà scattare ulteriori azioni se usate KDE come interfaccia grafica. Per i dispositivi che vengono usati per la prima volta, viene proposto un modulo di YaST ai fini della configurazione o inizializzati delle applicazioni da utilizzare con il nuovo dispositivo. Questo meccanismo viene eseguito in parallelo ad altre azioni che vengono azionati da `/etc/hotplug/usb.agent`.

I dispositivi USB vengono trattati dall'usb.agent in base al tipo:

Dispositivi di memorizzazione: come il disco rigido che appena sono stati caricati i driver necessari vengono gestiti dallo script `/usr/sbin/checkhotmounts`

Dispositivi di rete: essi generano un proprio evento hotplug nel kernel, non appena vengono rilevati. L'`usb.agent` mette a disposizione le informazioni hardware che saranno utilizzati dall'evento di rete. Si tratta di una soluzione provvisoria per il kernel 2.4 e fallisce se vengono utilizzati diversi dispositivi di rete USB, il che comunque si verifica di rado.

Camere: vengono indirizzate dalla scansione hardware/meccanismo di KDE. Bisogna a riguardo impostare i permessi di accesso del file di dispositivo per l' utente che è entrato nel sistema in `/etc/hotplug/usb/usbcam` affinché possa accerdervi sotto KDE.

Mouse: necessitano solo di un modulo caricato per poter essere utilizzati immediatamente che viene caricato a questo punto.

Tastiera: sono già necessari al momento del boot e per questo non vengono gestiti dall'hotplug.

ISDN/Modem attualmente non vengono configurati automaticamente.

Vi sono inoltre delle variabili specifiche per USB in `/etc/sysconfig/hotplug`. In ⟨*HOTPLUG_USB_HOSTCONTROLLER_LIST*⟩ avete i driver per il controller USB nella sequenza nella quale si cercherà di caricarli. Quando un driver è stato caricato, in ⟨*HOTPLUG_USB_MODULES_TO_UNLOAD*⟩ vengono registrati i moduli che saranno scaricati quando verrà rimossa la componente. Tutti i seguenti moduli per USB non vengono scaricati perché non può essere determinato con certezza se non sono ancora necessari per qualche dispositivo. La variabile ⟨*HOTPLUG_USB_NET_MODULES*⟩ contiene il nome dei moduli che mettono a disposizione un'interfaccia di rete. Non appena uno di questi moduli viene caricato, la descrizione dell'hardware viene deposta per l'uso futuro presso l'evento di rete. Questo processo viene protocollato nel systemlog.

PCI e PCMCIA

Nel caso di schede PCMCIA bisogna distinguere, dato che fatta eccezione per schede CardBus l'hotplug non gestisce alcuna scheda PC; e nel caso della scheda CardBus solo se il sistema PCMCIA del kernel è abilitato. Per saperne di più leggete, nel capitolo dedicato a PCMCIA, il paragrafo software (xxPCMCIA-SOFTWARExx).

Le schede CardBus sono da un punto di vista tecnico simile ai dispositivi PCI. Per questo entrambi vengono gestiti dallo stesso script hotplug `/etc/`

`hotplug/pci.agent` che soprattutto determina e carica il driver per la scheda. Inoltre viene indicato dove la nuova scheda è stata collegata (Bus PCI/slot PCMCIA e numero dello slot), affinché un successivo evento di rete hotplug possa leggere questa informazione e scegliere la giusta configurazione. L'assegnazione del driver avviene in due passaggi: come primo si cercano le impostazioni individuali nel file `/etc/hotplug/pci.handmap` e se non si trova niente, si cerca nella tabella PCI del kernel `/lib/modules/`⟨*versione del kernel*⟩`/modules.pcimap`. Chi dunque volesse modificare l'assegnazione dei driver, deve intervenire su `/etc/hotplug/pci.handmap`, poiché l'altra tabella viene sovrascritta all'aggiornamento del kernel.

Diversamente dagli USB non vengono eseguite delle particolari azioni a seconda del tipo di schede PCI o CardBus. Nel caso di schede di rete, il kernel genera un evento di rete hotplug che comporta la configurazione dell'interfaccia. Nel caso di tutte le altre schede, le azioni devono essere eseguite manualmente. Ma il sistema hotplug viene ottimizzato sotto questo punto di vista.

Appena viene rimossa una scheda, vengono scaricati anche i moduli utilizzati. Se a questo punto dovessero sorgere dei problemi, si possono ovviare scrivendo i nomi di modulo in `/etc/sysconfig/hotplug` nella variabile ⟨*HOTPLUG_PCI_MODULES_NOT_TO_UNLOAD*⟩.

Rete

Appena un'interfaccia di rete viene registrata o rimossa nel kernel, questi genera un evento di rete hotplug che viene analizzato da `/etc/hotplug/net.agent`. Al momento vengono analizzati solo interfacce Ethernet, Tokenring e WirelessLAN. Per tutti gli altri tipi di interfacce come modem o ISDN vi sono altri meccanismi. Le interfacce di rete messe a disposizione da schede PCMCIA e non dall'hotplug sono gestiti dal cardmanager. Il relativo messaggio appare nel systemlog.

Innanzitutto si determina quale hardware viene messo a disposizione dall'interfaccia. Visto che il kernel 2.4 non fornisce questo tipo di informazione viene utilizzata l'informazione messa a disposizione da un precedente evento hotplug USB o PCI. Anche se in linea di massima questo porta al risultato desiderato, bisogna considerarla una soluzione provvisoria, poiché non sarà possibile connettere contemporaneamente due schede di rete. Se usate più schede di rete hotplug, collegatele una dopo l'altra al computer in un intervallo di pochi secondi. La trasmissione di questa informazione viene protocollata in `/var/log/messages`.

Con l'informazione sul hardware viene richiamato lo script `/sbin/ifup` (o `ifdown`). ifup riesce ad assegnare ad una determinata scheda sempre la giusta

configurazione, anche nel caso in cui l'interfaccia ha un nome diverso, anche perché i nomi dell'interfaccia non vengono assegnati in modo mirato dal kernel.

Ulteriori azioni che intendete eseguire dopo che è stata creata un'interfaccia di rete possono essere annesse in `/sbin/ifup`. I dettagli sono reperibili nella pagina di manuale di `ifup` (`man ifup`). Sussiste anche la possibilità di usare diverse route default a secondo dell'hardware connesso, vedi la pagina di manuale di `route` (`man route`).

Se fallisce il tentativo di rilevamento automatico dell'hardware connesso all'interfaccia (per esempio il caso di Firewire) e si usa solamente un dispositivo di rete hotplug, allora la descrizione dell'hardware di rete può essere scritto in `/etc/sysconfig/hotplug` nella variabile ⟨*HOTPLUG_NET_DEFAULT_HARDWARE*⟩. La successione di caratteri deve corrispondere a quello che `/sbin/ifup` deve usare per la corretta configurazione. Nella variabile ⟨*HOTPLUG_NET_TIMEOUT*⟩ viene stabilito per quanto tempo `net.agent` attende la descrizione hardware generata dinamicamente.

Firewire (IEEE1394)

Per dispositivi Firewire al momento vengono caricati solo i moduli driver. Per vedere quanto diffuso è il Firewire tra i nostri clienti, contattate il nostro web front-end per il feedback `http://www.suse.com/feedback`.

Altri dispositivi e ulteriori sviluppi

Tutti i tipi di hardware hotplug che non stati menzionati in questa sede, al momemto non vengono (ancora) supportati. L'hotplug al momento si trova in una fase di sviluppo dinamico che dipende molto dalle funzionalità del kernel. Ci si può aspettare che con il kernel 2.6 la situazione su questo fronte migliorerà.

Notebook – PCMCIA, APM, IrDA e SCPM

Ai notebook vengono rivolte particolari richieste, devono disporre tra l'altro dell' Advanced Power Management (APM), interfacce ad infrarossi (IrDA) e schede PC (PCMCIA). A volte queste componenti sono presenti anche su computer da scrivania e visto che in questi casi le differenze sono minime rispetto ai notebook, l'uso e la configurazione di questi componenti - sia per PC da scrivania che per notebook - vengono trattati in questo capitolo .

PCMCIA

PCMCIA sta per “Personal Computer Memory Card International Association” ed indica hardware e software in relazione con questa associazione.

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 conviene 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 care. Dato che la velocità di trasmissione viene limitata in altri punti, nella maggioranza dei casi non conviene sobbarcarsi di lavoro aggiuntivo. Per queste schede sono disponibili intanto numerosi driver che però sono a volte poco stabili – in relazione anche del controller PCMCIA.

Quale scheda viene utilizzata, 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 l’ultima versione del PCMCIA-HOWTO.

La seconda componente necessaria è il controller PCMCIA è oppure il PC-Card/CardBus-Bridge che crea la connessione tra scheda e PCI-Bus e nei dispositivi anche tra scheda e ISA-Bus. Questi controller sono quasi sempre Intel-Chip i82365 compatibile. Vengono supportati tutti i comuni modelli. Il tipo di controller si lascia stabilire anche con il comando `probe`. Se si tratta di un dispositivo PCI, il comando `lspci -vt` fornisce informazione interessanti.

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 e così anche quello maggiormente collaudato e viene sviluppato ulteriormente ancor oggi. I sorgenti dei moduli utilizzati non sono incorporati 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 formano il sistema PCMCIA kernel. 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 il sistema. Per fare ciò nel file `/etc/sysconfig/pcmcia` alle variabili ⟨*PCMCIA_SYSTEM*⟩ va assegnato il valore `external` o `kernel` e bisogna riavviare PCMCIA con `rcpcmcia restart`. Per un cambio temporaneo potete utilizzare anche `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 pacchetto `pcmcia` e `hotplug`.

All'avvio di PCMCIA vengono caricati i moduli `pcmcia_core`, `i82365` (PCMCIA esterno) o `yenta_socket` (PCMCIA kernel) e `ds` che inizializzano i controller PCMCIA e mettono a disposizione le funzioni di base Raramente al posto di `i82365` o `yenta_socket` viene richiesto il modulo `tcic`. .

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 dallo gestore della 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. (Vedi anche capitolo *Hotplug* a pagina 207).

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 trova in `/etc/pcmcia`. Quelli per l'hotplug in `/etc/hotplug`. Se si stacca 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 della 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 quali script ha utilizzato il demone ai fini della configurazione. Teoricamente una scheda PCMCIA può essere staccata facilmente. 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 e eseguire correttamente l'unmount che chiaramente non sarà più possibile una volta staccata la scheda. In caso di dubbio aiuta un

```
cardctl eject
```

Con questo comando disattivate tutte le schede che si trovano nel notebook. Per disattivare solo una delle schede, indicate in aggiunta il numero dello slot, per esempio `cardctl eject 0`

La configurazione

Attraverso il runlevel editor di YaST oppure con `chkconfig` nella riga di comando potete determinare se avviare la 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 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 di `pcmcia_core` (`man pcmcia_core`).

⟨***PCMCIA_PCIC_OPTS***⟩ contiene dei parametri per il modulo `i82365`. Anche in questo caso vi è una su pagina di manuale di `i82365` (`man i82365`). Se utilizzate `yenta_socket`, queste opzioni vengono ignorate, poiché `yenta_socket` non riconosce 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 `pcmciaD` (`man pcmciaD`) trovate i dettagli sulla sintassi di questi file.

La correlazione tra driver e schede PCMCIA per hotplug viene descritta nel capito sull'hotplug (vd. *Hotplug* a pagina 207).

Schede di rete (Ethernet, Wireless LAN e TokenRing)

Queste schede 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 incentrato sulla rete. 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 vengono trattati come 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 soft modem. Generalmente non sono supportati. Se esistono dei driver, vanno integrati singolarmente 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.

Nota

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 ad girare stabilmente.

Nota

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 un init-ramdisk (initrd) ; per ulteriori informazioni vedi la sezione *Il boot con l'initial ramdisk* a pagina 275. initrd contiene un file system virtuale, con tutti i necessari moduli e programmi PCMCIA. Il bootdisk o le immagini del bootdisk contengono le stesse cose, 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*.

Configurare lo switch – SCPM

Spesso su computer portatili si ha bisogno di diversi profili di configurazione, per il lavoro o per uso domestico. Con dispositivi PCMCIA grazie agli schemi PCMCIA questo non è stato mai problema. Dato che comunque anche gli utenti di schede di rete integrate fisse o di dispositivi USB/FireWire vogliono utilizzare diversi profili per la configurazione del sistema, a partire da SuSE Linux 8.0 vi è il pacchetto SCPM (System Configuration Profile Management). Per questo motivi supporta SuSE lo schema PCMCIA. Chi comunque desidera utilizzare questo schema, deve adattare manualmente la configurazione sotto `/etc/pcmcia`. Noi consigliamo l'uso di SCPM, poiché potete gestire qualunque aspetto della configurazione del sistema non solo quelli relativi alla PCMCIA.

La documentazione su SCPM si trova nella sezione *SCPM – System Configuration Profile Management* a pagina 225.

Problemi

Finora utilizzando 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 manualmente di moduli bisogna considerare una particolarità. I due sistemi PCMCIA utilizzano moduli omonimi e risiedono in diverse sottodirectory sotto `/lib/modules/`⟨*versione del kernel*⟩. Questi 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 attraverso `insmod /lib/modules/`⟨*versione del kernel*⟩/⟨*sottodirectory*⟩/⟨*nome file del modulo*⟩ o con `modprobe -t` ⟨*sottodirectory*⟩ ⟨*nome_del_modulo*⟩.

Attenzione

Innanzitutto si deve scoprire se il problema dipende dalla scheda, o se il problema è causato dal sistema di base PCMCIA. Così il computer va in ogni caso avviato inizialmente 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 il testo necessario. Così le possibili cause di errore - descritte di seguito - si lasciano ridurre a due.

Non funziona il sistema di base PCMCIA

Se il sistema al boot si ferma al messaggio PCMCIA: "Starting services", 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 con i comandi

`terra:~ #` **`modprobe -t`** ⟨***dir***⟩ **`pcmcia_core`**

`terra:~ #` **`modprobe -t pcmcia-external i82365`** (con PCMCIA esterno)

oppure

`terra:~ #` **`modprobe -t pcmcia yenta_socket`** (con PCMCIA kernel)

oppure – in casi rarissimi –

`terra:~ #` **`modprobe -t`** ⟨***dir***⟩ **`tcic`**

e

`terra:~ #` **`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 `pcmcia_core`. Le opzioni ivi descritte possono essere testate con il comando modprobe. Come esempio disabiltiamo il supporto APM dei moduli PCMCIA; a volte possono verificarsi 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` nella 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 utilizzati più opzioni, separateli da uno spazio:

```
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` (`man i82365`).

Il problema in questi casi è dovuto ad un conflitto di risorse, interrupt, porta IO o l'area della memoria viene occupata due volte. Il modulo `i82365` controlla queste risorse prima di renderle disponibili ad una scheda, a volte però proprio questo controllo è la causa del problema. Infatti il controllo dell'interrupt 12 (dispositivi PS/2) comportano un blocco del mouse e/o tastiera. In questi casi è d'aiuto il parametro `irq_list=`⟨*ElencodegliIRQ*⟩. L'elenco deve contenere tutti gli IRQ che possono essere utilizzati. Dunque

```
modprobe i82365 irq_list=5,7,9,10
```

o in modo duraturo 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 connesse sotto config.opts non vengono utilizzate per una scheda PCMCIA, ma che comunque vengono controllati dal modulo di base i82365.

Non funziona (bene) la scheda PCMCIA

Qui esistono in linea di massima tre varianti: 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 considerare se la scheda viene amministrata dal gestore di schede o dall'hotplug. Ricordatevi: con PCMCIA esterno reagisce 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. Problemi con l'hotplug verranno trattati nel capito sull'hotplug (vedi capitolo *Hotplug* a pagina 207).

- **La schede non viene riconosciuta.**
  Se la scheda non viene riconosciuta, appare in `/var/log/messages` 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 scoprire come la scheda si presenta. Ulteriori informazioni nel PCMCIA-HOWTO sezione 6 e nella pagina di manuale di `pcmcia` (`man 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 correlazione errata che per esempio può essere dovuto al fatto, che un fornitore abbia integrato in un modello di schede 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 vengono 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'assegnazione delle risorse del sistema possono essere visualizzati con `lsdev`. (Può capitare 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/`⟨*corretta directory pcmcia*⟩`/`⟨*driver*⟩ (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. Consiglio: `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 correntemente 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 per esempio 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 è stata configurata in modo errato**
  In questp 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 tra degli script di rete, assegnando in `/etc/sysconfig/network/config` alla variabile `DEBUG=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.

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 coi moduli.

Dopo il boot dal dischetto (oppure dopo aver selezionato 'l'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 selezionato la voce 'Carica moduli PCMCIA'. Dapprima appaiono due campi di immissione dove poter immettere le opzioni per i moduli `pcmcia_core` `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`.

Secondo lo stato attuale delle cose con SuSE Linux 8.1 si installa come sempre con il sistema PCMCIA esterno. Se dopo la stesura di questo manuale ciò dovesse cambiare, lo riconoscerete dal fatto che non vengono richiesti delle opzioni di moduli per `i82365` e che invece viene utilizzato il modulo `yenta_socket`. Durante l'installazione i messaggi del sistema vengono emessi su diverse console virtuali, su cui si può accedere con (Alt) + (tasto funzione). Quando l'interfaccia grafica è attivata, con (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 vi è una bash e tanti comuni strumenti di sistema.

Se durante l'installazione viene caricato un errato modulo driver 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 da 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 *Problemi* a pagina 218 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.

Ulteriori tool

E' stato menzionato più volte il programma `cardctl`. cardctl è il tool principale per ottentere delle informazioni da PCMCIA o per eseguire delle determinate operazioni. In cardctl trovate ulteriori dettagli, o immettendo `cardctl` otterrete un elenco di comandi validi.

Per questo comando vi è un frontend grafico `cardinfo` (cfr. Fig. 8.1 nella pagina seguente), con cui controllare le funzioni principali. Comunque pacchetto `pcmcia-cardinfo` deve essere installato.

Figura 8.1: *Il programma cardinfo*

Ulteriori tool nel pacchetto `pcmcia` sono `ifport`, `ifuser`, `probe` e `rcpcmcia` che comunque non sono sempre necessari. Per sapere precisamente cosa contiene il pacchetto `pcmicia`, eseguite il comando `rpm -ql pcmcia`.

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 in 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.

Ulteriori informazioni

Chi è interessato a certi notebook, dovrebbe visitare ad ogni caso l'home page laptop di Linux all'indirizzo: `http://linux-laptop.net`. Un'ulteriore buona fonte di informazione è la home page Moblix sotto: `http://mobilix.org/` (MobiliX – Mobile Computers and Unix). Troverete oltre a tante utili informazioni anche un laptop-Howto ed un IrDA-Howto. Inoltre vi è nella banca dati di supporto l'articolo Laptops and Notebooks (PCMCIA) on Linux `http://sdb.suse.de/en/sdb/html/laptop.html` (o localmente sotto `file:/usr/share/doc/sdb/de/html/laptop.html`).

SCPM – System Configuration Profile Management

A volte si rende necessario - dovuto a diverse ragioni - 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, oppure 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 egreggiamente solo per l'hardware PCMCIA, ove era possibile avere degli schemi che contenevano diverse configurazioni. Sulla base di tale principio abbiamo sviluppato SCPM ("System Configuration Profile Management" che non si limita solo a componenti PCMCIA. Con il cosiddetto "System Configuration Profile Management" potete stabilire liberamente una parte della configurazione del sistema di cui i diversi stati debbano essere riportati 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.

L'area di applicazione principale sarà la configurazione di rete dei portatili. Comunque, diverse impostazioni di rete influiscono anche su altri elementi per esempio le impostazioni per posta elettronica o proxy, o stampanti diverse a casa e in ufficio, la configurazione XFree86 per il beamer colari impostazioni per il risparmio energetico durante gli spostamenti o un diverso fuso orario rispetto alle 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 costruire SCPM su di una struttura di base flessibile così da permettere per esempio 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.com/feedback` (preferibilmente in inglese).

Terminologia e principi

Ecco la terminologia usata di seguito per descrivere SCPM usata anche nel modulo di YaST.

- *Configurazione del sistema* riguarda le principali impostazioni per esempio 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 e i vostri meta-dati, ovvero utente, permessi o tempo di accesso; si può trattare anche di un servizio di sistema una volta abilitato e spento in un altro profilo.
- Le risorse vengono raccolte in cosiddetti *Gruppi di risorse*. I 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.

Modulo YaST2 per SCPM e ulteriore documentazione

Quale front-end grafico per SCPM (pacchetto `scpm`) vi è un modulo di YaST (il pacchetto `yast2-profile-manager` da poter usare come alternativa 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`). Nella console si usa `info` o `pinfo`. La documentazione tecnica per coloro che vogliono sperimentare con SCPM si trova sotto `/usr/share/doc/packages/scpm`. `scpm` senza ulteriori argomenti elenca i vari comandi.

Configurare SCPM

Prima di iniziare a lavorare con SCPM bisogna abilitarlo. Di solito SCPM viene utilizzzato 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 della riga di comando devono venir eseguiti come utente *root*. Potete abilitare o disabilitare i gruppi tramite `scpm activate_group NOME` e `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 può durare un 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.

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 per esempio 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 contenente 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; cioècon `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 per esempio `work` in `lavoro` e per cancellarlo di seguito, immettete `scpm rename work lavoro` e poi `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'.

Passare da un profilo di configurazione all'altro

Come abbiamo visto sopra nel caso di `work` si usa il comando `scpm switch work`. 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 ciò riguarda solo un piccola parte del sistema mentre la parte rimanente del sistema continua a funzionare.

Solo a questo punto vengono

1. fermati i servizi di sistema,
2. salvate tutte le risorse modificate (per esempio file di configurazione) e
3. (ri)avviati i servizi del sistema.

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

```
\befehl{scpm} \wert{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`, cioè 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*⟩ e `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 `""`; cioè cioè `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` oppure `scpm get prestop work`.

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 utilizzato il nome del profilo per l'opzione `title`. GRUB è il bootloader di default. Una descrizione dettagliata si trova nella sezione *Boot con GRUB* a pagina 77; oppure immettete `info grub`. La configurazione di GRUB sarà per esempio:

```
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
```

file 26: *Il file /boot/grub/menu.lst*

Per i sistemi che utilizzano LILO utilizzate il file 27 .

```
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"
```

file 27: *Il file /etc/lilo.conf*

Ora al momento del boot potete scegliere comodamente il profilo che desiderate.

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 aggiornamento 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 il problema che SCPM si interrompa durante il passaggio da un profilo all'altro. Ciò può essere dovuto a motivi esterni - p.e. 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: modificare la configurazione dei gruppi di risorsa con SCPM in esecuzione in linea di massima non crea delle difficoltà. Dovete badare che dopo aver aggiunto o eliminato dei gruppi, invocate `scpm rebuild` che aggiunge nuove risorse a tutti i profili e cancella quelle eliminati. Quest'ultime saranno cancellate in modo definitivo; se li avete configurati 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 modificata da SCPM. Se modificate la configurazione con YaST, non è necessario un comando rebuild, YaST lo eseguirà automaticamente.

APM e ACPI – il power management

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 (ingl. *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. Se siete in possesso di un portatile con una implementazione APM funzionante, usatela, perché vi sono sempre più case produttrici

che non utilizzano più APM e implementano il più recente standard ACPI (ingl. *Advanced Configuration and Power Interface*). ACPI è più complesso e presuppone una stretta collaborazione tra case produttrici di hardware, programmatori BIOS ed esperti di sistemi operativi. Inoltre l'implementazione ACPI non è ancora pronta per il kernel Linux e per questo utilizzabile solo in parte. Bisogna aspettare il kernel 2.6 prima di registrare dei miglioramenti su questo fronte.

Funzionalità per il risparmio energetico

Queste funzioni sono di interesse per tutti, ma di particolare importanza 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) L'intero 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 svegli dallo stato di ibernazione e per tornare precisamente a quello stato antecedente all'ibernazione. Alcune case produttrici offrono nel loro APM un variante interessante (per esempio RediSafe dei Thinkpads di IBM). Questa funzione corrisponde allo stato S4 dell'ACPI. Anche per Linux esiste una simile soluzione software non contenuta però in SuSE Linux. Chi la volesse usare deve porre mano da sé: `http://sourceforge.net/projets/swsusp/`

Controllo dello stato della batteria Oltre a controllare lo stato di caricamento della batteria, bisogna agire quando le riserve di energia stanno per esaurirsi. Anche qui entrano in gioco le routine BIOS dell'APM. Potete inoltre usare come alternativa `apmd/acpid` o `klaptopdaemon`.

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 disattivati via ACPI almeno in teoria temporaneamente o permanentemente nel Bios setup. Soprattutto la porta a infrarossi dovrebbe essere possibilmente spenta finché non sia necessaria, vedi la sezione *IrDA – Infrared Data Association* a pagina 246.

Controllo dell'attività del processore Con APM spesso vi è solo la possibilità di scegliere nel BIOS setup tra diverse impostazioni. Per determinati dispositivi vi sono tool speciali per controllore queste impostazioni che interessano l'hardware, p.es. per IBM Thinkpads `tpctl` e `apmiser` del pacchetto `tpctl`. Potete controllare la frequenza del processore con il programma `procspeed` del pacchetto `apmd`. Le prestazioni del processore possono essere direttamente influenzati tramite l' ACPI, quindi ne parleremo nella sezione dedicata all'ACPI.

APM

Alcune funzionalità di risparmio energetico vengono eseguite autonomamente dal BIOS APM. Spesso 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 installare i relativi pacchetti ed il kernel adatto.

Nei kernel di SuSE Linux il supporto APM è integrato e viene attivato automaticamente non appena al boot venga rilevato un BIOS APM. Con `apm=off` al prompt di boot potete disattivare il supporto APM. 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 gli 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 (real mode).

(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*⟩ Tempo in 1/100 di secondo con i quali determinare l'(in)attività del sistema.

Il demone APM (apmd)

Il demone `apmd` vigila sullo stato della batteria e può far scattare delle determinate azioni se si entra nella modalità stand-by o suspend. Lo trovate nel pacchetto 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 limitiremo 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 viene fermato il disco fisso. I valori possibili vengono descritti nella sezione *Un breve intervallo per il disco rigido* a pagina 245 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 limite massimo per i dati nel buffer.

APMD_BATTERY/AC_FILL_LEVEL Il livello 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 `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 ed essere riaccese 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 per esempio la velocità di ripetizione dei tasti o l'orario dopo la sospensione, o di far 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.

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` (`man 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 almenokpanel –, può visualizzare lo stato di caricamento della batteria anche con kbatmon e sospendere ogni attività del sistema. Alternativamente è di sicuro interesse anche xosview.

ACPI

Principi

ACPI sta (ingl. *Advanced Configuration and Power Interface*). ACPI permette al sistema operativo di configurare e controllare le singole componenti di hardware. In tal maniera ACPI sostituisce sia il plug 'n play che l' APM. La parte dell'ACPI che inizializza l'hardware non verrà descritta in questo capitolo. Non vi sono neanche dei margini di manovra per l'utente.

Il BIOS mette a disposizione delle tabelle in cui trovate delle informazioni sulle singole componenti e sui metodi di accedere all'hardware. Il sistema operativo utilizza queste informazioni per assegnare per esempio degli interrupt oppure per accendere e spegnere delle componenti. Visto che il sistema operativo esegue istruzioni che si trovano nel BIOS anche qui dipende molto dalla implementazione del BIOS. In `/var/log/boot.msg` trovate i messaggi di boot. Lì ACPI indica quali tabelle ha rilevato e letto.

DSDT Differentiated System Description Table: contiene delle informazioni sulle componenti del computer e sul modo di configurarle.

FADT Fixed ACPI Description Table: contiene delle informazioni sull'implemetazione del blocco di registro hardware ACPI e tra l'altro l'indirizzo fisico della DSDT.

MADT Multiple APIC Description Table: descrive l'implementazione e la configurazione dell' APIC.

RSDT Root System Description Table: Tabella dei puntatori su altre tabelle. Quello su RSDT (RSDP) deve trovarsi in un settore di memoria basso.

SSDT Secondary System Description Table: questa tabella è la continuazione della DSDT. Possono esservi più SSDT. La suddivisione in più tabelle aumenta il grado di flessibilità soprattutto per l'OEM.

XSDT Extended Root System Description Table: Contiene le identiche informazioni della RSDT, può però contenere anche dei puntatori su description header di oltre 32 bit. L'RSDP può puntare anche su XSDT

Lo standard ACPI definisce numerosi stati di sistema. Ecco quelli principali:

G0 Sistema è in esecuzione

G1 Sistema dorme, passaggio a G0 senza dover avviare l' OS (Suspend)

G2 Soft off, OS deve avviarsi all'accensione

G3 Spento meccanicamente (interruttore principale), nessuna alimentazione

Vi sono poi 6 stati di dormiveglia per distinguere ulteriormente G0/G1/G2:

S0 Sistema è in esecuzione

S1 Standby (basso consumo di corrente, ma il sistema si risveglia velocemente)

S2 Un'altra forma di standby che però spesso non viene implementata nei dispositivi.

S3 Suspend (bassissimo consumo di corrente con risveglio veloce)

S4 Ibernazione o suspend to disk (nessun consumo di corrente, risveglio più lento (tra 20 e 100 secondi, a seconda dell'hardware)

S5 Soft off (G2)

Inoltre vi sono per ogni componente hardware gli stati D0 - D3 in cui le singole componenti sono attive, sospese o spente. Vi sono anche degli stati particolari del processore per determinate stati del sistema. Gli stati C vengono introdotti da comandi CPU su cui non è possibile intervenire direttamente:

C0 Processore è in esecuzione

C1 Processore esegue particolari istruzioni pausa che richiedono meno energia ma che comunque permettono di riprendere subito il lavoro.

C2 Come C1 con ancor meno consumo energetico ma maggior tempo per il risveglio.

C3 Come C2 con ancor maggior risparmio, ma la cache di primo livello diventa inconsistente (implementato solo in pochi dispositivi e usato di rado).

Gli stati della performance dipendono dalle caratteristiche dei processori come Speedstep (Intel) o PowerNow (AMD). Si interviene sulla frequenza di clock e tensione del core della CPU:

P0 massima frequenza di clock e massima tensione della CPU

P1 primo livello di risparmio, vengono ridotte la frequenza e la tensione

P2 prossimo livello di risparmio (se esistente)

P3 ...

Il throttling è la terza possibilità in questo contesto: si interrompe temporaneamente la velocità di clock della CPU:

T0 0% riduzione di clock

T1 12% riduzione di clock

T2 25% riduzione di clock

T4 ...

Gli stati P e T possono essere impostati direttamente dall'utente (o tramite demone). La differenza principale riguarda il risparmio energetico. Con il throttling si realizzano solo dei risparmi lineari, p.es. 25% di riduzione del clock corrisponde ad una riduzione del 25% della performance e 25% meno consumo (solo del processore). Mentre se si modifica la performance a causa della tensione ridotta vi è un maggior risparmio rispetto al calo della performance. Spesso si riduce la performance come mezzo per il "raffreddamento passivo", mentre quello attivo si ha con la ventola. Questa alternativa è interessante se durante l'uso del computer volete accorciare i tempi per ricaricare la batteria del portatile.

Inoltre l'ACP fornisce delle informazioni su batteria, alimentatore, temperatura e ventola, e segnala inoltre eventi di sistema per esempio "Abbassa monitor" o " Batteria quasi vuota".

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.

Dopo bisogna caricare una serie di moduli per l'OSPM ("Operating System Power Management"). Questi vengono caricati dallo script di avvio del demone di ACPI. Se uno di questi moduli dovesse creare dei problemi, in `/etc/sysconfig/powermanagement` 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` trovate una serie di dati che vi informano sullo stato del sistema o grazie alle quali è possibile modificare attivamente lo stato. Comunque alcune delle funzionalità si trovano nello stato sperimentale o non sono state implementate dal produttore. Tenete presente:

Attenzione

Con ACPI non funziona ancora né suspend to RAM né to disk (ibernazione). Queste funzioni ci saranno solo a partire della versione del Kernel 2.6 (o. 2.5 per gli smanettoni tra di voi). Chi vuole, può integrare nel kernel la patch "sw-susp". Vedi funzione di risparmio energetico: ibernazione.

Attenzione

Tutti i file (tranne `dsdt` e `fadt`) possono essere letti con `cat`. In alcuni si possono modificare le impostazioni 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 Con
`echo anno-mese-giorno ora:minuto:secondo > /proc/acpi/alarm`
stabilite quando si debba risvegliare il sistema. Visto che però attualmente non funzionano gli stati di ibernazione non ha senso impostare l'ora di risveglio.

/proc/acpi/sleep Informa sui possibili stati di ibernazione. Qui sarà possibile innescare un suspend, per ora funzionano solo S1 (standby) e S5 (spegni subito, ma la procedura di shutdown non è delle più corrette): 'echo 1 > /proc/acpi/sleep'.

/proc/acpi/event Qui vengono indicati tutti gli eventi che vengono elaborati da un demone come 'acpid' o 'ospmd'. Se non vi accede alcun demone, gli eventi possono essere visualizzati con 'cat /proc/acpi/event' (terminare con Ctrl-C), per esempio se si preme brevemente l'interruttore o se si abbassa il monitor.

/proc/acpi/dsdt e /proc/acpi/fadt Qui trovate le tabelle ACPI: DSDT e FADT 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 si ricorre 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/CPU0/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/CPU0/performance Questa interfaccia non viene più utilizzata. Vedi la sezione *Speedstep oppure PowerNow* a pagina 243.

/proc/acpi/processor/CPU0/throttling Qui è possibile un ulteriore throttling lineare del processore.

/proc/acpi/processor/CPU0/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. Con `echo 1:5 > /proc/acpi/processor/CPU0/limit` non saranno utilizzati gli stati P0 o rispettivamente T0-T4.

/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 sono 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 dell'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 completamente 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 temperatura viene 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 syslog. 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 (in inglese) sotto `http://www.suse.de/feedback`.

Speedstep oppure PowerNow

I processori per dispositivi mobili adattano il clock del processore alle attuali condizioni di sistema. L'interfaccia di sistema per questa tecnologia è stata estrapolata dall'ACPI. Sotto `/proc/cpufreq` e `/proc/sys/cpu/0/speed*` trovate i valori ammessi ed potete impostare la frequenza. Per maggiori dettagli consultate `/usr/src/linux/Documentation/cpufreq/`.

Il demone cpufreqd adatta la frequenza del processore automaticamente alle attuali condizione di sistema. Questo demone non viene inizializzato automaticamente al boot del sistema. Per avere maggiori informazioni riguardo l'avvio di servizi di sistema consultate la sezione *L'editor dei runlevel editor di YaST* a pagina 305. La documentazione su cpufreqd si trova in `/usr/share/doc/packages/cpufreqd/README.SuSE` e nella pagina di manuale (`man cpufreqd`. Le impostazioni si eseguono in `/etc/sysconfig/powermanagement`.

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 modifiche (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 dovuti 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 vengono risolte in tal maniera in modo molto efficace. 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 semplice delle risorse.

acpi=off non utilizzare ACPI.

Analizzate in questi casi i messaggi di boot, utilizzate a riguardo per esempio il comando `dmesg | grep -2i acpi` (o tutt 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. Comunque questo non è semplice da realizzare e serve l'aiuto di esperti. Per alcuni computer vi sono delle DSDT corrette su Internet.

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 cercano 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:

- `http://www.columbia.edu/~ariel/acpi/acpi_howto.txt` (ACPI HowTo un pò datato e incompleto)
- `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://codecs.home.sapo.pt/acpi/index.html` (ACPI patch)
- `http://www.poupinou.org/acpi/` (DSDT Patch di Bruno Ducrot)
- `http://sourceforge.net/projects/cpufreqd` (Il progetto Linux CPUFreq)

- http://sourceforge.net/projects/swsusp (Ibernazione del kernel: progetto "swsusp")
- Mailing list: lister.fornax.hu/pipermail/swsusp

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 impostare in vario modo il 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. ⟨*x*⟩ 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 e 241 fino a 251 corrispondono a 1 fino a 11 volte 30 minuti.

Spesso però non è facile stabilire dei valori, visto che sotto Linux vi sono numerosi processi che salvano i dati sul disco e quindi "svegliano" continuamente il disco. 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 nel buffer della RAM. Il buffer viene controllato del "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 è riempito del 30%. Allora il demone bdflush scrive i dati sul disco. A volte li scrive sul disco anche indipendentemente da kupdated se per esempio il buffer è pieno. Chi è in possesso di un sistema stabile può modificare queste impostazioni, però deve tenere conto che ne va della sicurezza dei dati.

Le impostazioni si lasciano visualizzare con cat /proc/sys/vm/bdflush. Il primo valore indica il livello a partire dal quale viene svuotato il buffer. Il sesto valore indica la permanenza massima dei file consentita, espressa in centesimi di secondo. Il quinto valore indica l'intervallo entro il quale kupdated controlla il buffer, espresso anche in centesimi di secondo. Per avere per esempio un intervallo kupdated di 1 minuto, utilizzate il seguente comando:

```
echo 30 500 0 0 6000 > /proc/sys/vm/bdflush
```

I valori che precedono il valore da modificare sono semplicemente da copiare, i valori che seguono il valore da modificare possono essere omessi.

Così se immettete

```
echo 60 > /proc/sys/vm/bdflush
```

vuol dire che il livello da raggiungere prima che il buffer venga svuotato è - espresso in percentuale - del 60%. Gli altri valori vengono descritti nei sorgenti del kernel nel file `Documentation/filesystems/proc.txt`.

Attenzione

Sicurezza dei dati esposta

Modificare le impostazioni del demone di aggiornamento del kernel (ingl. kernel update daemon) influisce anche sulla sicurezza dei dati. In caso di dubbio non modificate alcunché.

Attenzione

Le impostazioni per il timeout del disco, 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 sull'apmd *Il demone APM (apmd)* a pagina 235 e nei file.

Oltre a quanto descritto fin qui, anche i cosiddetti "Journaling File system" per esempio ReiserFS o Ext3 scrivono indipendentemente da `bdflush` i loro meta-dati 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 state utilizzando. Per esempio buoni editor di testi scrivono di nascosto sul disco delle copie di sicurezza del file appena modificato. Queste funzionalità si lasciano comunque disabilitare, ma bisogna sempre tener conto della sicurezza dei dati.

In questo contesto vi è per il demone di posta elettronica `postfix` una variabile `POSTFIX_LAPTOP` che se impostata su `yes`, postfix riduce notevolmente il numero degli accessi al disco. Comunque diventa trascurabile se l'intervallo per `kupdated` è stato esteso.

IrDA – Infrared Data Association

IrDA ("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 avvia 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://mobilix.org/Infrared-HOWTO/Infrared-HOWTO.html` e sul home page del Linux IrDA Project `http://irda.sourceforge.net/`.

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`.

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, poiché ad intervalli brevissimi (pochi 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

```
rcirda start
```

Potete attivare in ogni momento le interfacce manualmente o disattivarle (con il parametro `stop`). Attivando 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.

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 la luce infrarossa.

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 si trovi 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, wireless ad Internet servendovi del programma wvdial. Potete anche alineare 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 negli output di irdadump vengono indicati nella parentesi quadra dopo i nomi dei dispositivi. Il 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 su Linux.

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:

```
irdadump
```

Nel caso di una stampante Canon BJC-80 nei pressi del computer si ha un output simile al seguente ripetuto più volte (cfr. output 14).

```
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)
```

output 14: *IrDA: irdadump*

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 è 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.

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 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 convenzioni di chiamata (ingl. *calling conventions*) aggiornate delle funzioni si realizza una maggiore performance.

Questa edizione di SuSE Linux supporta il nuovo processore in due modi:

- I 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

SuSE Linux a 64 bit per AMD64

Hardware

Sul lato hardware AMD64 non si distingue dagli atri 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.

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. Questo consente soprattutto di installare RPM a 32 bit senza dover apportare delle modifiche.

OpenOffice ed alcuni pacchetti commerciali come ad esempio Acrobat Reader non sono pacchetti a 64 bit.

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.

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
```

Sviluppo software sotto i 64 bit

Su SuSE Linux per sistemi AMD64 è possibile sviluppare sia programmi a 32 bit che a 64 bit. l compiler GNU di solito creano un codice AMD64 a 64 bit. Con `-m32` si ha la creazione 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.

Ulteriori informazioni

Per ulteriori informazioni rimandiamo al sito web di AMD (`www.amd.com`) e la pagina dei progetti riguardanti il porting Linux su AMD64 (`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 vostro kernel. 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 stato sperimentale".

Per creare un nuovo kernel, vi sono dei `makefile`, grazie ai quali il processo è si svolte in modo quasi completamente 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.

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 *Boot e boot manager* a pagina 73.

Per installare il kernel originale di SuSE Linux 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`.

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 (pacchetto `gcc`), i binutils GNU (pacchetto `binutils`) ed i file include per il compiler C (pacchetto `glibc-devel`) vengono installati automaticamente.

I sorgenti del kernel si trovano nella directory `/usr/src/linux-<versionedelkernel>.SuSE` Se avete in mente di fare qualche esperimento con il kernel e volete averne contemporaneamente diverse versioni sul disco rigido, 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.

Configurazione del kernel

La configurazione del kernel impostato durante l'installazione o l'update viene archiviata nel file`/boot/vmlinuz.config`. Se intendete modificare la configurazione del kernel, andate come `root` nella directory `/usr/src/linux` ed eseguite il comando `make oldconfig` che genera un file `.config` oppure eseguite il comando riportato di seguito:

```
cp /boot/vmlinuz.config /usr/src/linux/.config
```

Come alternativa potete anche utilizzare la configurazione del kernel attualmente in esecuzione. Sotto SuSE Linux immettete in questo caso

```
zcat /proc/config.gz > /usr/src/linux/.config
```

I tool di configurazione del kernel leggeranno questo file `.config`. La config-

urazione del kernel può essere eseguita in tre modi diversi: dalla riga di comando, tramite un menù in modo testo oppure sotto l'X Window System. Le tre possibilità verranno descritte brevemente.

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, ci sono normalmente due o tre possibilità di risposta: o un semplice (y) e (n), o una delle tre possibilità (y) (ingl. *yes*), (n) (ingl. *no*) e (m) (ingl. *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.

Configurazione nel modo testo

Per una configurazione più comoda, usate "menuconfig"; eventualmente dovete installare il pacchetto `ncurses-devel` con YaST. Iniziate la configurazione del kernel con il comando `make menuconfig`.

Non dovrete rispondere a "centinaia" di domande, 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.

Configurazione sotto l' X Window System

Se avete installato l'X Window System (il pacchetto `xf86`) e Tcl/Tk (il pacchetto `tcl` e il pacchetto `tk`), potete, in alternativa, eseguire la configurazione con

```
make xconfig
```

Avrete a disposizione una interfaccia grafica che rende più confortevole la configurazione. Per farlo, però, dovrete aver inizializzato l' X Window System

come utente `root` o aver già immesso nella shell `xhost +` come utente normale, per permettere a `root` di accedere allo schermo. I valori di default vengono letti dal file `.config`. Tenete presente che conviene sempre, per ragioni varie, dopo `make xconfig` di eseguire `make oldconfig`.

Non dimenticate dopo aver modificato la configurazione di ricreare le dipendenze. Indipendentemente dal metodo di configurazione alla fine date questo comando:

```
make dep
```

Questo è necessario soprattutto se intendete compilare dei moduli di kernel per software commerciale.

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") indirizza 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.

Quali driver sono parte integrante del kernel e quali saranno presenti sotto forma di moduli viene stabilito al momento della configurazione del kernel. 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 analoghe vanno compilati direttamente nel kernel, mentre il supporto per `isofs`, `msdos` o `sound` dovrebbe essere compilato come modulo.

I moduli del kernel vengono archiviati nella directory `/lib/modules/`⟨*versione*⟩; ⟨*versione*⟩ corrisponde alla versione attuale del kernel.

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.

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 più venire usato in favore di `modprobe` (vedi sotto).

- `rmmod`
  Elimina il modulo indicato. Ciò è naturalmente consigliabile solo se la corrispondente funzione del kernel non viene più usata. Non è, 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.e. 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 sono attualmente caricati da quanti altri moduli vengono usati. I moduli caricati dal demone del kernel sono contrassegnati con `(autoclean)`; ciò significa che questi moduli vengono automaticamente rimossi se non sono vengono usati per un certo periodo di tempo. Vedi però in questa pagina.

- `modinfo`
  Vi mostra i dettagli di un modulo.

Il file /etc/modules.conf

Il caricamento dei moduli dipende inoltre dal file `/etc/modules.conf`; cfr. la pagina di manuale di `depmod` (`man depmod`).

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 pacchetto `kernel-source` e leggete la relativa documentazione che trovate nella directory `/usr/src/linux/Documentation`.

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 impostato per scaricare automaticamente dei moduli; con la quantità di RAM dei computer odierni, il guadagno in termini di RAM sarebbe trascurabile; vedi anche `/usr/src/linux/Documentation/kmod.txt`. Per server che devono eseguire solo compiti speciali e che necessitano solo pochi driver si consiglia, per ragioni di prestazione, un kernel "monolitico".

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 pacchetto `kernel-source`.

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:

```
make dep
make clean
make bzImage
```

Potete inserire questi 3 comandi anche in una riga di comando:

```
make dep clean bzImag
```

Alla fine della compilazione, troverete il kernel compresso nella directory `/usr/src/linux/arch/i386/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
```

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

```
befehlmake 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.

Suggerimento

Assicuratevi di eliminare da `/lib/modules/"`⟨*versione*⟩ i moduli, le cui funzioni sono state integrate nel kernel, per evitare conseguenze imprevedibili. Per questo motivo, sconsigliamo *vivamente* alle persone inesperte di compilarsi un kernel da sé.

Suggerimento

Affinché GRUB 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 un etichetta Linux.old come immagine di boot. Questo procedimento viene spiegato dettagliatamente nel capitolo *Boot e boot manager* a pagina 73. 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` o `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`.

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 e particolarità del caricamento con "initrd", il programma linuxrc ed il "Sistema di salvataggio".

Gli standard Linux

Filesystem Hierarchy Standard (FHS)

SuSE Linux cerca di conformarsi al *Filesystem Hierarchy Standard* (FHS, il pacchetto `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.

Linux Standard Base (LSB)

SuSE supporta il progetto *Linux Standard Base*; per informazioni attuali, vd. `http://www.linuxbase.org`.

Il sistema attuale supporta la specificazione LSB nella versione 1.3.x; il Filesystem Hierarchy Standard (FHS) è ormai parte integrante della specificazione, che determina anche il formato dei pacchetti e l'inizializzazione del sistema; cfr. capitolo *Il concetto di "boot"* a pagina 297.

teTeX – TeX su SuSE Linux

TEX è un programma per scrivere testi che gira su numerose piattaforme. E' estendibile tramite macro-pacchetti come LATEX. E' composto da numerosi file, impostate secondo la *TEX Directory Structure* (TDS) (cfr. `ftp://ftp.dante.de/tex-archive/tds/`) teTeX è una raccolta di software TEXaggiornato.

Su SuSE Linux, teTeX viene usato nella configurazione che debba soddisfare i requisiti della TDS e dell' FHS.

Esempi di ambienti per FTP ed HTTP

Su FTP

Per facilitare l'allestimento di un server FTP, il pacchetto `ftpdir` offre un esempio di ambiente, da installare su `/srv/ftp`.

Su HTTP

Apache è il server web standard di SuSE Linux; assieme all'installazione, vi vengono messi a disposizione dei documenti-esempio sotto `/srv/httpd`. Se volete allestire un proprio server web, registrate il vostro DocumentRoot in `/etc/httpd/httpd.conf` e archiviate lì i vostri file (documenti, immagini etc.).

Informazioni su pacchetti speciali di software

Il pacchetto bash ed /etc/profile

Quando richiamate una shell di login i file di inizializzazione vengono analizzati da bash in questa sequenza:

1. `/etc/profile`
2. `~/.profile`
3. `/etc/bash.bashrc`
4. `~/.bashrc`

Gli utenti possono eseguire alcune registrazioni in `~/.profile` o `~/.bashrc`. Per garantire un'elaborazione corretta dei file è necessario che le impostazioni basilari di `/etc/skel/.profile` o `/etc/skel/.bashrc` vengono assunte dalla 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`.

Il pacchetto cron

Le tabelle cron si trovano su `/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 28, che indica `root`); i dati dei pacchetti su `/etc/cron.d` hanno lo stesso formato – cfr. pagina di manuale di `cron` (`man 8 cron`).

```
1-59/5 * * * * root test -x /usr/sbin/atrun && /usr/sbin/atrun
```

file 28: *Esempio di valori di /etc/crontab*

`/etc/crontab` *non* può essere modificato con `crontab -e`, ma deve venire direttamente caricato in un editor, modificato, e infine memorizzato.

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`. `/usr/lib/cron/run-crons` viene richiamato ogni 15 minuti dalla tabella principale (`/etc/contrab`); in questo modo, si assicura che vengano recuperate per tempo esecuzioni mancate.

Gli interventi di manutenzione quotidiani sul sistema sono stati distribuiti su diversi script per motivi di chiarezza. (Pacchetto pacchetto `aaa_base`). in `/etc/cron.daily` oltre a `aaa_base` vi è per esempio `backup-rpmdb`, `clean-tmp` o `clean-vi`.

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 log file o file di protocollo, 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 aumenta di giorno in giorno. Con l'aiuto del pacchetto `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. pagina di manuale di `logrotate` (`man 8 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 valutati; su SuSE Linux è previsto che i singoli pacchetti di `/etc/logrotate.d` installino dei file (ad esempio, `syslog` o `yast`).

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#    monthly
#    create 0664 root utmp
#    rotate 1
#}

# system-specific logs may be also be configured here.
```

file 29: *Esempio di /etc/logrotate.conf*

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 che avreste potuto eseguire come amministratore nei file `/etc/permissions*`. Assicuratevi sempre che le vostre modifiche non creino dei conflitti.

Nota

Pagine di manuale

Per alcuni programmi GNU (per esempio tar), le manual page non vengono più aggiornate. Al loro posto, troverete un sommario nell'edizione `--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` Facili da usare sono anche `tkinfo`, `xinfo` o il sistema d'aiuto.

Il comando ulimit

Con il comando `ulimit` (ingl. *user limits*), potrete limitare l'accesso all'uso delle risorse del sistema o visualizzare le risorse. `ulimit` è particolarmente adatto a ridurre 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` in modi diversi Per limitare l'uso di memoria, usate le opzioni riportate nella tabella 11.1.

`-m`	grandezza massima della memoria fisica
`-v`	grandezza massima della memoria virtuale (swap)
`-s`	grandezza massima dello stack
`-c`	grandezza massima dei core file
`-a`	visualizzazione dei limiti impostati.

Tabella 11.1: `ulimit`*: impostare le risorse dell'utente*

Le impostazioni 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`.

```
# Limite della memoria reale:
ulimit -m 98304

# Limite della memoria virtuale:
ulimit -v 98304
```

file 30: *Impostazioni ulimit su ~/.bashrc*

La memoria viene espressa in KB.

Per informazioni più dettagliate, consultate pagina di manuale di `bash` (`man bash`).

Nota

Non tutte le shell supportano le indicazioni `ulimit`. Se non potete fare a meno di questo tipo di restrizioni, PAM (per esempio `pam_limits`) offre ampie possibilità di impostazione.

Nota

Il comando free

Il nome del comando `free` è un pò fuorviante, dal momento che questo comando serve a verificare quanta memoria venga attualmente usata…

Troverete le informazioni essenziali su `/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 a quando non vi erano ancora sistema di gestione unitari della memoria (ingl. *unified memory management*). Il motto di Linux è: *la memoria libera è cattiva memoria* (ingl. *free memory is bad memory*), il che vuol dire che Linux cerca sempre di bilanciare le varie cache, ma di non lasciare mai della memoria del tutto inutilizzata (o libera)

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. pagina di manuale di `mmap` (`man 2 mmap`)).

Inoltre, il kernel dispone anche di altre memorie temporanee, come la cosiddetta "slab cache", che contiente anche un buffer usato per le connessioni alla rete. Così si spiegano tutte le differenze tra i denominatori di `/proc/meminfo`. La maggior parte delle cache (ma non tutte) possono essere consultate attraverso `/proc/slabinfo`.

Il file /etc/resolv.conf

La risoluzione del nome viene gestita tramite il file `/etc/resolv.conf`; cfr. sezione *DNS – Domain Name System* a pagina 344.

Il file `/etc/resolv.conf` viene continuamente attualizzato solo dallo script `/sbin/modify_resolvconf`. A nessun programma è permesso modificare `/etc/resolv.conf` direttamente. Solo così si può assicurare che la configurazione della rete ed i relativi dati rimangono consistenti.

Impostazioni per GNU Emacs

GNU Emacs è un ambiente di lavoro complesso; ulteriori informazioni sono reperibili sotto:

cfr. `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 quando 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` garantisce che vengano caricate automaticamente dei file di configurazione speciali, che vengono installati con i pacchetti aggiuntivi di Emacs della distribuzione (per esempio 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 pacchetto `emacs-x11` che contiene il programma *con* supporto per l'X11.
- In pacchetto `emacs-nox` trovate il programma *senza* supporto per X11.
- Il pacchetto `emacs-info`: 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: pacchetto `emacs-auctex` (per LaTeX); pacchetto `psgml` (per SGML/XML); pacchetto `gnuserv` (per uso client/server) etc.

Il boot con l'initial ramdisk

Problematiche

Non appena il kernel di Linux è caricato e il file system root(`/`) ha eseguito il mount, 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 se SCSI), il kernel ha bisogno dei driver corrispondenti. Inoltre, il kernel deve contenere il codice necessario a 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 un gran numero di kernel differenti, ed in più la presenza di diversi kernel ottimizzati (ottimizzazione Pentium, SMP, ecc.).

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.

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.

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. Quando linuxrc ha concluso, l'`initrd` (temporaneo) viene "smontato" (ingl. *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` richiede il nome speciale di `linuxrc` e di trovarsi nella directory root di `initrd`. Inoltre, deve essere eseguito dal solo 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`.

Bootloader

La maggioranza dei bootloader (soprattutto GRUB, LILO e syslinux) sono in grado di usare `initrd`. Ecco i singoli bootloader:

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 ⟨altri parametri⟩
```

L'impiego di initrd con SuSE

Installazione del sistema

`initrd` viene usato già da parecchio tempo per l'installazione: l'utente può caricare moduli 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`, si chiude, e il processo di boot del kernel continua nel sistema appena installato.

In un'installazione di SuSE Linux, si esegue quindi il boot del sistema che in pratica si sta installando. Un vero riavvio dopo l'installazione avviene solo se il kernel in esecuzione non si sposa bene con i moduli che sono stati installati nel sistema. Dacché SuSE Linux, al momento dell'installazione, usa un kernel per sistemi monoprocessore, ciò avviene solo quando nel sistema sia stato installato un kernel SMP assieme ai relativi moduli. Per poter usare tutti i moduli, si deve perciò caricare il kernel SMP che è appena stato installato nel sistema.

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 certo tipo di 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 e successivo di ulteriori driver SCSI è problematico (come potrebbe venire inizializzato se anche sul secondo adapter SCSI vi sono collegati dei dischi rigidi?), carichiamo tutti i driver SCSI usati durante l'installazione tramite `initrd`.

Importante: poiché il caricamento di `initrd` tramite il bootloader viene eseguito este come il caricamento del kernel stesso (LILO annota nel suo file `mappa` la locazione dei file), dopo ogni modifica di `initrd`, si deve reinstallare LILO! Se utilizzate grub questo non è necessario.

Possibili difficoltà – kernel auto-compilati

Se compilate un kernel spesso può subentrare il seguente problema: per abitudine, il driver SCSI viene integrato nel 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 da un altro contesto (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` e rispettivamente da `/etc/grub/menu.lst` cosa che produce lo stesso effetto come eliminare il driver da INITRD_MODULES ed immettere `mkinitrd`, che, a sua volta, constaterà che non è necessario alcun `initrd`.

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 `/`.

- Driver EIDE soghigh end
- 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`
- `/usr/src/linux/Documentation/initrd.txt`
- La pagina di manuale di `initrd` (`man 4 initrd`).

linuxrc

linuxrc è un programma che viene inizializzato durante la fase di avviamento del kernel e prima che venga fatto il boot. Questa proprietà del kernel permette di caricare un piccolo kernel modulare e, successivamente, le unità di disco veramente necessarie sotto forma di moduli. programmlinuxrc vi aiuta a caricare le unità di disco necessarie al vostro hardware. Normalmente, tuttavia, ci si può affidare tranquillamente dell'identificazione automatica dell'hardware, eseguita da YaST prima dello start. Potete usare linuxrc sia per l'installazione, che come strumento di caricamento di un'altro sistema installato. Potete persino avviare un sistema autonomo di salvataggio basato sul ramdisk, per informazioni dettagliate consultate la sezione *Il sistema di salvataggio SuSE* a pagina 285.

Menù principale

Dopo aver impostato e la tastiera, avrete accesso al menù principale di linuxrc (vedi Figura *Menù principale di linuxrc* a pagina 11). Di norma, si usa linuxrc per avviare Linux. Il nostro obiettivo è pertanto la voce del menù 'Installazione/Avviare sistema'. Che riusciate ad accedere a questa voce direttamente, dipende dall'hardware del PC e dalla portate dell'installazione; per maggiori approfondimenti, consultate il paragrafo *L'installazione in modo testo con YaST* a pagina 8.

Impostazioni

Potete ora impostare 'Lingua', 'Schermo' (colori/bianco e nero), 'Tastiera' e 'Debug (Esperti)'.

Informazioni sul sistema

Su 'Informazioni sul sistema' (figura *Informazioni sul sistema* in questa pagina), oltre ai messaggi del kernel, troverete gli indirizzi I/O delle schede PCI, la capacità della memoria principale riconosciuta dal Linux e altro.

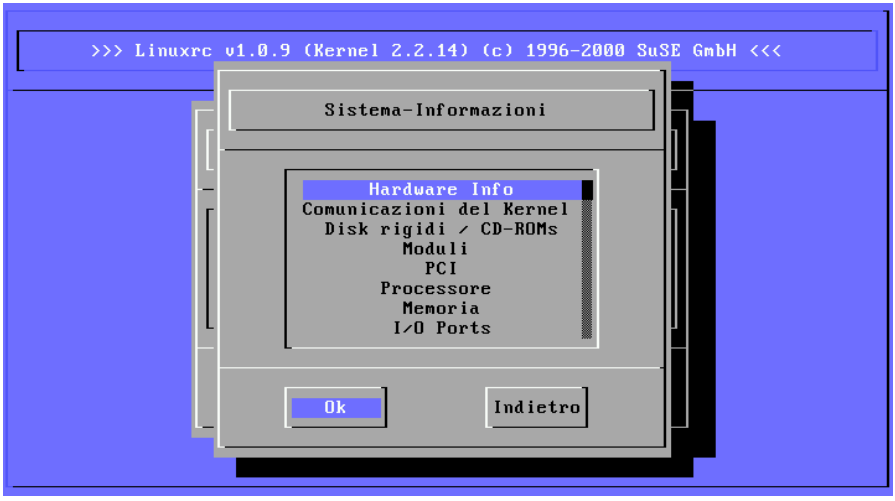


Figura 11.1: *Informazioni del sistema*

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 integrata un'unità di disco SCSI, non sarà naturalmente più necessario caricare moduli 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 >
```

Caricare i moduli

Scegliete il tipo di modulo di cui avete bisogno. Se avete fatto il boot dal dischetto, linuxrc leggerà i dati e vi metterà a disposizione un'ampia gamma di moduli. Se avete caricato dal CD o se avete eseguito un "poststart" da DOS tramite loadlin, tutti i moduli sono già a disposizione di linuxrc. Questo risparmia un lungo caricamento, ma in compenso necessita più memoria.

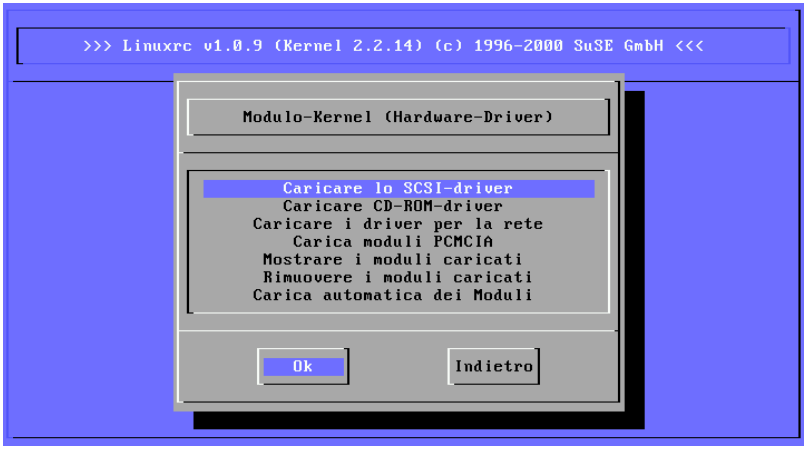


Figura 11.2: *Caricare i moduli*

linuxrc vi offre un elenco di unità di disco disponibili. A sinistra, trovate il nome del relativo modulo; a destra, una breve descrizione dell'hardware per cui l'unità è competente.

Per alcuni componenti possono esserci più driver o driver alpha recenti. Anche quest'ultimi vi vengono offerti.

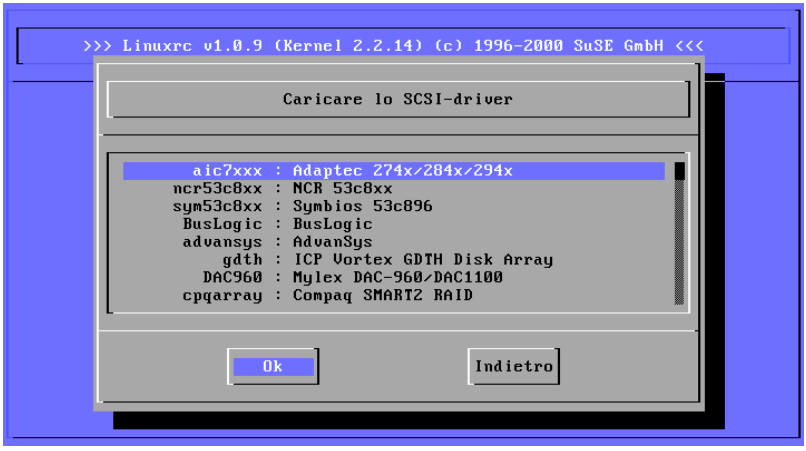


Figura 11.3: *Scelta dei driver per SCSI*

Inserimento dei parametri

Una volta trovata l'unità di disco corrispondente al vostro hardware, posizionate il cursore e premete ↵. A questo punto appare una maschera in cui poter digitare i parametri del modulo da caricare. A questo punto vogliamo ricordarvi che, al contrario del prompt del kernel (MILO, LILO o SYSLINUX), qui più parametri per uno stesso modulo devono essere separati da uno spazio vuoto.

In molti casi non è necessaria l'esatta specificazione dell'hardware; la maggior parte delle unità disco trova da sola i suoi componenti. Solo schede di rete e dispositivi CD-ROM un pò più datati potrebbero necessitare dei parametri. In ogni caso, provate prima con ↵.

Con alcuni moduli, il riconoscimento e l'inizializzazione dell'hardware possono durare a lungo. Passando alla console virtuale 4 (Alt + F4), potrete leggere i messaggi di caricamento del kernel. Gli 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.

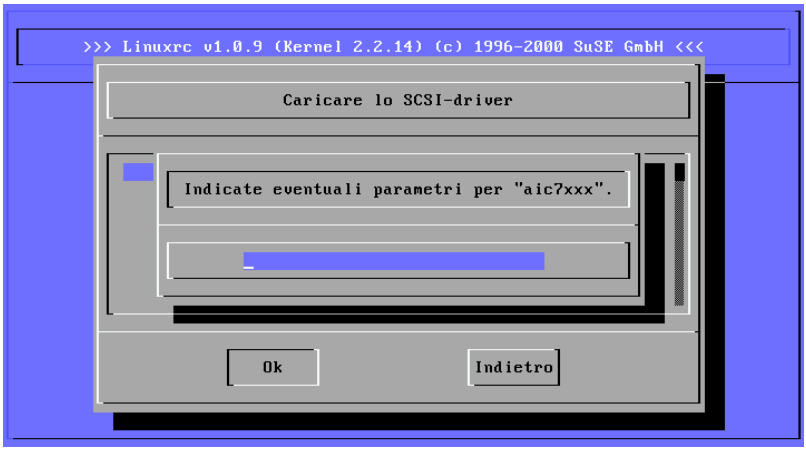


Figura 11.4: *Digitazione dei parametri per il caricamento dei moduli*

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 (Figura *Avvia l'installazione* a pagina 13) è possibile inizializzare diversi processi: 'Avviare installazione/update', 'Caricare sistema installato' (la partizione root deve essere nota), 'Inizializzare sistema di salvataggio' (vd. sezione *Il sistema di salvataggio SuSE* nella pagina successiva) e 'Espelli CD'.

Se avete fatto il boot da un cosiddetto "LiveEval-CD", avrete ora anche il punto 'LiveEval-Avvia CD'. Potete scaricare delle image ISO dal server FTP (`live-eval-`⟨*VERSION*⟩):

`ftp://ftp.suse.com/pub/suse/i386/`

Suggerimento

Il punto 'Inizializzare il Live-CD' può sempre essere utile se si vuole provare, *senza* fare un'installazione sul disco rigido, se il computer o il notebook sono compatibili con SuSE Linux. Dovreste essere in grado di eseguire questo tipo di test da un qualsiasi rivenditore di PC.

Suggerimento

Per l'installazione (figura *Inizializzare il sistema / l'installazione* a fronte), come anche per il sistema di salvataggio, potete scegliere diversi dispositivi (Figura *Lanciare il sistema di salvataggio* a pagina 288).

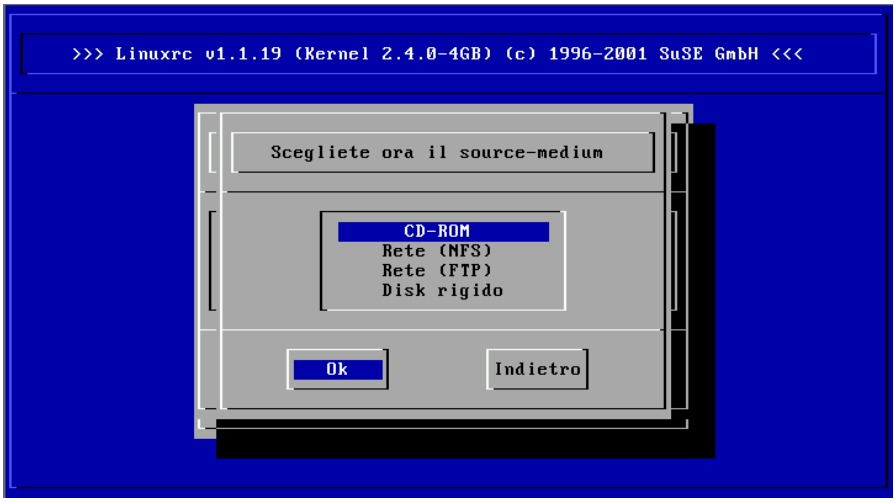


Figura 11.5: *Scelta del dispositivo d'installazione in linuxrc*

Il sistema di salvataggio SuSE

SuSE Linux contiene diversi sistemi di salvataggio con i quali in caso di necessità si può accedere dall'"esterno" alle proprie partizioni Linux, tramite per esempio *dischetto di avviamento* e il sistema di *"salvataggio"* che potrete caricare dal dischetto, CD, rete o server FTP della 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 ad accedere, file di configurazione errati etc. Parted (`parted`) ne è una componente con cui potete 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/`

Suggerimento

Create sempre un dischetto di avvio e ripristino, ne vale la pena anche in termini di fatica e tempo che vi risparmierete nel caso per un motivo qualsiasi non fosse più possibile utilizzare il lettore di CD-Rom.

Suggerimento

Preparativi

Per creare il vostro sistema di salvataggio vi servono due dischetti: uno come dischetto di avvio e l'altro per contenere l'immagine compressa di un piccolo file system root. Il file immagine `bootdisk` per l'avvio del sistema e il file `rescue` per il file system root lo trovate sul primo CD sotto `boot`.

Vi sono tre possibilità per creare il dischetto con il file system root:

- con YaST
- tramite una console e comandi Linux

```
terra:~ #  /sbin/badblocks -v /dev/fd0 1440
terra:~ #  dd if=/media/cdrom/boot/rescue of=/dev/fd0 bs=18k
```

- tramite il prompt di DOS (con `Q:` per designare il lettore di CD-Rom)

```
Q:\> cd \dosutils\rawrite
Q:\dosutils\rawrite> rawrite.exe
```

Il dischetto di salvataggio si basa attualmente su libc5 (SuSE Linux 5.3), dato che in questa versione di SuSE Linux è possibile che alcuni programmi come per esempio editor, fdisk o e2fsck vengano copiati su un dischetto.

Nota

Il dischetto di salvataggio non si lascia montare, perché non si tratta di un file system ma solo di un'immagine compressa di un file system. Se volete vedere il file system, seguitate a leggere questo paragrafo.

Nota

Se volete avere un'immagine non compressa dovete decomprimere il file immagine e montare l'immagine decompressa come utente `root`. Se il vostro kernel supporta il *loop-device*, dovete immettere:

```
terra:~ #  cp /media/cdrom/boot/rescue /root/rescue.gz
terra:~ #  gunzip /root/rescue.gz
terra:~ #  mount -t ext2 -o loop /root/rescue /mnt
```

Lanciare il sistema di salvataggio

Il sistema di salvataggio viene avviato da un dischetto del boot SuSE creato in precedenza o da un CD o DVD atto al boot. La premessa è che il lettore dei dischetti, CD/DVD sia atto al boot; se necessario dovete modificare nella configurazione del CMOS dovete modificare la sequenza di avvio.

Ecco i passi da seguire per avviare un sistema di salvataggio:

1. Inserite il vostro dischetto di avvio SuSE (`bootdisk`) o primo CD o DVD von SuSE Linux nel relativo drive e accendete il vostro sistema.

2. Ora, potete lasciar fare il boot al programma o selezionare 'Manual Installation', nonché, se necessario, impostare dei parametri alla voce 'boot options'. Vi mostreremo anche come determinare quali moduli del kernel caricare.

3. Impostate lingua e tastiera su linuxrc.

4. Nel menù principale scegliete 'Inizializzare l'installazione/il sistema'.

5. Se avete fatto lo start con il *dischetto di boot*, inserite ora il CD per l'installazione o il dischetto (`rescue`) con la copia compressa del sistema di salvataggio.

6. Nel menù 'Inizializzare l'installazione/il sistema', scegliete il punto 'Inizializzare il sistema di salvataggio' (vd. figura *Avvia l'installazione* a pagina 13) e indicate il dispositivo sorgente desiderato (figura *Lanciare il sistema di salvataggio* nella pagina successiva):

   Alla fine, un paio di indicazioni per le possibilità di scelta:

   'CD-ROM': quando caricate il sistema di salvataggio, il percorso `/cdrom` viene esportato. In questo modo diventa possibile installare da *questo* CD.

   'Rete': per avviare il sistema `rescue` tramite una connessione di rete. Avrete bisogno anche dell'unità di disco della scheda di rete; cfr. le informazioni generali nel paragrafo *Installazione tramite "rete"* a pagina 17. In un sottomenù, troverete una serie di protocolli (vd. fig. 11.7 a pagina 289): NFS, FTP, SMB, ecc.

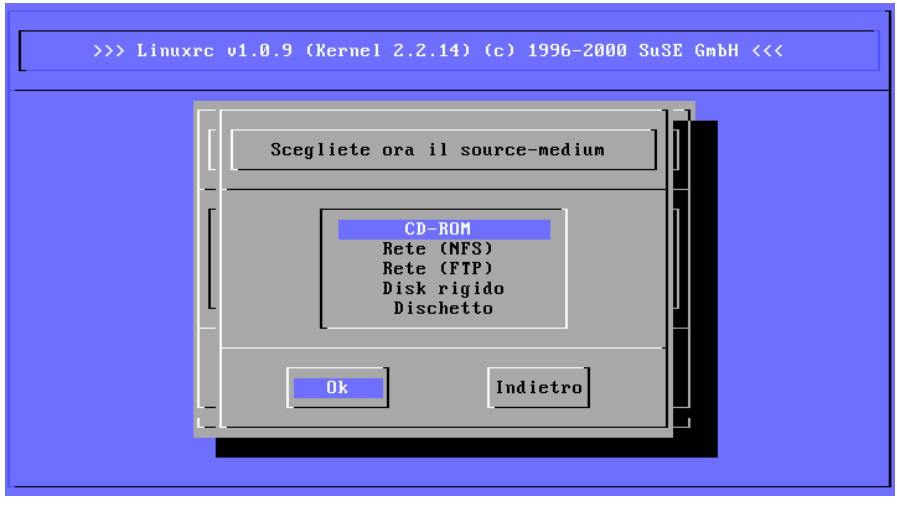


Figura 11.6: *Il mezzo sorgente del sistema di salvataggio*

'Disco rigido': per caricare il sistema `rescue` dal disco rigido.

'Dischetto': inizializzare il sistema `rescue` dal dischetto, soprattutto quando il computer ha poca RAM a disposizione.

Il sistema di salvataggio viene decompresso, caricato, montato e inizializzato in un disco RAM come nuovo file system root. Ora è pronto per l'uso.

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 fare 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 finestra di comando e l'utility (p.e. mount); una certa quantità di file-utility e utility di rete, fra cui e2fsck, per controllare e riparare i file system, 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 l'uso della rete, come ifconfig, route e netstat.

Il vostro editor del caso è vi che trovato sotto `/usr/bin`; qui troverete anche altri tool: (grep, find, less etc.) come pure telnet.

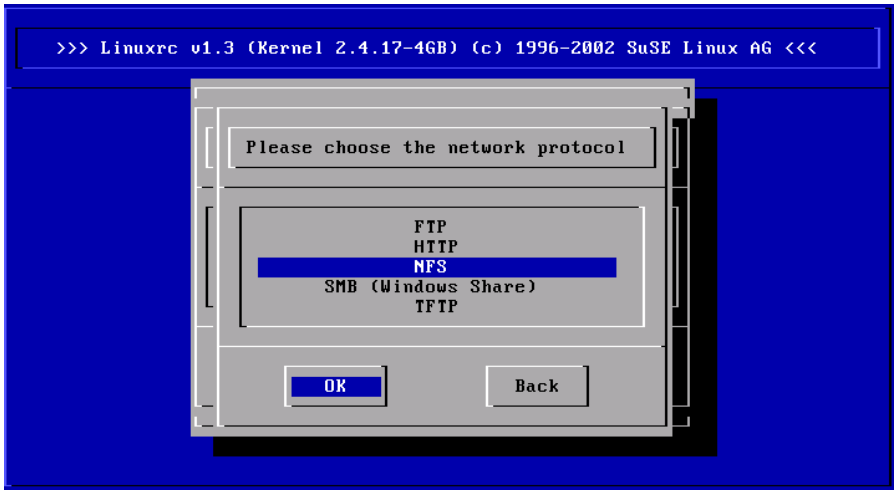


Figura 11.7: Protocolli di rete

Accesso al sistema normale

Per montare il vostro sistema Linux sul disco rigido, abbiamo 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 comunichi che il vostro sistema presenti la composizione del file-esempio *Accesso al sistema normale* in questa pagina.

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

file 31: *Esempio /etc/fstab*

Attenzione

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

Attenzione

Montatelo quindi passo per passo sotto `/mnt` con i seguenti comandi (rispettate la sequenza!):

```
terra:/ #  mount /dev/sdb3 /mnt
terra:/ #  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 su `/mnt/etc` invece che su `/etc`!).

Perfino partizioni che erano andate completamente perse, si possono recuperare (ovvero ricreare) con Linux fdisk; si deve però sapere esattamente in quale punto del disco rigido si trovavano prima le partizioni.*Ogni* esperto utente di Linux archivia il più presto possibile uno stampato di `/etc/fstab` e uno stampato del comando

```
terra:~ #  fdisk -l /dev/⟨disk⟩
```

Al posto di ⟨*disk*⟩ inserite uno dopo l'altro i nomi dei dispositivi del vostro disco rigido, ad esempio `hda`.

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. I file system non possono venire riparati durante il normale uso del sistema. In presenza di danni gravi, potrebbe non essere possibile montare il file system root e l'avvio del sistema e l'avvio del sistema causare un "kernel panic". L'unica cosa da farsi a questo punto, è quella di provare ad eseguire la riparazione "da fuori" con un sistema di salvataggio.

Nel sistema di salvataggio di SuSE Linux sono contenuti gli strumenti 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 manual page di e2fsck, la trovate stampata nell'appendice *Manual-Page di e2fsck* a pagina 567.

Esempio: se un file system, a causa di un *Superblock non valido* non si lascia più montare, molto probabilmente, in un primo tempo, fallirà anche `e2fsck`. La soluzione consiste nell'usare uno dei superblock backup creati nel file system ogni 8192 blocchi (8193, 16385. . .). Ciò viene eseguito p.e. dal comando

```
terra:~ #  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 superblock, pensa che sia tutto a posto.

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 capacità.

In modo di testo sono a disposizione 6 console virtuali; premendo la combinazione di tasti (Alt) +(F1) fino a (Alt) +(F6), potete passare da una console all'altra. La settima console è riservata a X11. Modificando il file `/etc/inittab`, potete anche determinare il numero di console disponibili.

Se, da X11, volete ritornare su una console di testo senza però chiudere X11, usate la combinazione (Ctrl) +(Alt) +(F1) fino a (Ctrl) +(Alt) +(F6). Con (Alt) +(F7) ritornate a X11.

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/⟨VERSION⟩/site-lisp/term/*.el
/usr/lib/joerc
```

Queste modifiche si applicano solo alle applicazioni che leggono `terminfo`, o i cui file di configurazione sono stati direttamente modificati (`vi`, `less` etc.). Altre applicazioni non-SuSE devono venire adattate a queste impostazioni di default. Sotto X il tasto compose ("Multi_key") si ottiene tramite la combinazione (Ctrl) + (⇑) (destro); cfr. la registrazione in `/usr/X11R6/lib/X11/Xmodmap`.

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* e *localizzazione*: rispettivamente 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 (ingl. *native language support*), ma anche delle categorie per le *notizie* (linguaggio), *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 pagina di manuale di `locale` (`man 5 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.

   L'impostazione attuale può venire richiesta con il comando `locale`.

2. RC_LC_ALL: questa variabile soprascrive, 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 vengono impostate tramite l'editor `sysconfig`.

Il valore di tali variabili è composto dall'indicazione della lingua (ingl. *language code*), paese o territorio (ingl. *country code*), set dei caratteri (ingl. *encoding*) ed opzione (ingl. *modifier*). Le singole indicazioni vengono collegate ai caratteri speciali:

`LANG=`⟨*language*⟩`[[_`⟨*COUNTRY*⟩`].Encoding[@Modifier]]`

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. Un file di descrizione per it_IT@euro.UTF-8 viene creato con:

```
terra:~ #  localedef -i it_IT@euro -f UTF-8 it_IT@euro.UTF-8
```

LANG=it_IT.ISO-8859-1

Per la lingua italiano vale il set di caratteri ISO-8859-1 che inoltre contiene anche il simbolo dell'Euro; questo set di caratteri si usa se un programma non è stato ancora adattato ad ISO-8859-15.

L'indicazione del set di caratteri (qui ISO-8859-1) viene riconosciuta per esempio da Emacs.

LANG=it_IT@euro

Segue un esempio per settare una opzione (euro). Per impostare it_IT@euro il default per l' installazione standard è italiano.

LANG=it_IT.UTF-8

Se lavorate in un xterm Unicode, dovete indicare UTF-8. Se volete lanciare un xterm per UTF-8, si dovrebbe creare un semplice shell-script con il nome uxterm (per esempio); cfr. file 32.

```
#!/bin/bash
export LANG=it_IT.UTF-8
xterm -fn \
 -Misc-Fixed-Medium-R-Normal--18-120-100-100-C-90-ISO10646-1 \
 -T 'xterm UTF-8' $*
```

file 32: *uxterm per avviare un xterm Unicode*

SuSEconfig elenca le variabili /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 le predisposizioni del sistema in `~/.bashrc`. Se la predisposizione è `it_IT` e l'utente non è soddisfatto delle comunicazioni del programma in lingua tedesca, può cambiare e impostare la lingua inglese:

```
LC_MESSAGES=en_US
```

Adattamento per il supporto della lingua

Generalmente, per ottenere un fall back, i file delle categorie *Notizie* vengono archiviati solo nella directory della lingua (p.e. `de`). Se quindi LANG viene impostato su `de_AT` e se il file "Message" non è esistente sotto `/usr/share/locale/de_AT/LC_MESSAGES`, si ricorre a `/usr/share/locale/de/LC_MESSAGES`.

Con LANGUAGE è anche possibile determinare una "cascata" di fallback; p.e. per il bretone → francese o per il gallego → spangnolo → portoghese:

```
LANGUAGE="br_FR:fr_FR"
LANGUAGE="gl_ES:es_ES:pt_PT"
```

O – a seconda delle preferenze – utilizzare la variante 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, LC_TIME va trattato anche diversamente.

Problemi possibili

- Il punto delle cifre composte con 1.000 non viene riconosciuto. Probabilmente LANG si trova su `de`. Poichè 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*, cap. "Locales and Internationalization"; contenuto nel pacchetto `glibc-info`, serie `doc`.
- Jochen Hein [Hei96], 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*, attuale sotto `http://www.cl.cam.ac.uk/~mgk25/unicode.html`.
- *Unicode-Howto* di Bruno Haible `file:/usr/share/doc/howto/en/html/Unicode-HOWTO.html`.

Il 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); (cfr. la sezione *Linux Standard Base (LSB)* a pagina 268).

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.

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 "uccidere" 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 seguente, *I runlevel* in questa pagina) 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.

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. tabella 12.1 a pagina 300). Alternativamente, potrete impostare il runlevel desiderato durante il caricamento (per esempio al prompt di boot); il kernel passerà i parametri che non gli servono direttamente al processo init senza modificarli.

Per passare ad un altro runlevel in un secondo momento, basta chiamare 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

```
root@terra:/ >  init 1
```

si passa nel *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

```
root@terra:/ >  init 3
```

per avviare il sistema nel solito runlevel, nel quale si trovano tutti i programmi necessari al funzionamento del sistema e che permette di eseguire il login agli utenti. Con `init 0` oppure `shutdown -h now` potete spegnere il sistema e con `init 6` oppure `shutdown -r now` riavviarlo.

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

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 (es. NFS)*)
3	Modo multiutente completo con rete (ingl. *Full multiuser with network*)
4	Libero (ingl. *Not used*)

5	Modo multiutente completo con rete e KDM (standard), GDM o XDM (ingl. *Full multiuser with network and xdm*)
6	Riavvio del sistema (ingl. *System reboot*)

Tabella 12.1: *Elenco dei runlevel disponibili in Linux*

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' X Window System sia già stato configurato correttamente; (Capitolo *Il sistema X-window* a pagina 97). Verficate se il sistema funzione 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 di 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 LILO, 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

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 alla 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 la `'K'` (ingl. *kill*), mentre gli script di avvio iniziano con la `'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`, ne verifica la presenza di eventuali modifiche e, se necessario, adotta tutte le misure del caso (avviando, ad esempio, un `getty` su un'altra interfaccia).

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 l'utente 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`. Questo serve per aver maggior chiarezza ed 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 12.2.

Opzione	Significato
`start`	Avvia servizio
`stop`	Arresta servizio
`restart`	Arresta e riavvia servizio, se il servizio era già in esecuzione; altrimenti, avvia servizio
`reload`	Ricarica la configurazione del servizio senza fermarlo e riavvialo
`force-reload`	Ricarica la configurazione del servizio se il servizio supporta questa operazione. Altrimenti esegui un `restart`
`status`	Mostra stato attuale

Tabella 12.2: *Tabella sinottica delle opzioni degli script init*

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. pagina di manuale di `insserv` (`man 8 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 `devpts`, attivato il 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. chiamare 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 relativi allo schermo, finché `/var` non sia 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 possono 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` di DOS.

`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.

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

Script di inizializzazione personali

Degli errori negli script di inizializzazione possono bloccare tutto il 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 *I runlevel* a pagina 298.

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:

```
### 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
```

output 15: *Un INIT INFO minimale*

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. Gli script di avvio e di arresto nei runlevel vengono numerati in base a quanto indicato qui. 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 *L'editor dei runlevel editor di YaST* nella pagina successiva.

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.

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.

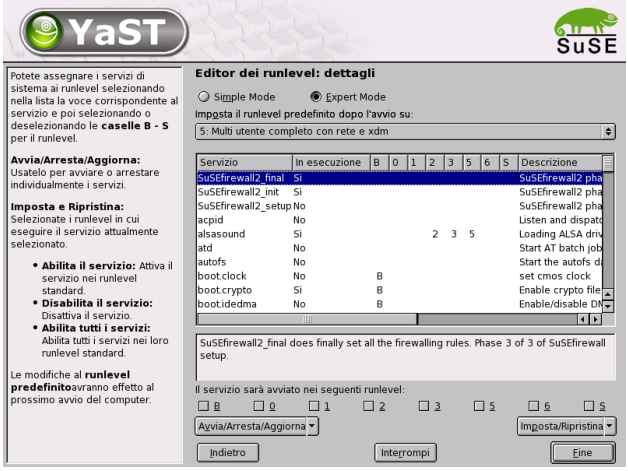


Figura 12.1: YaST: editor dei runlevel

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 per esempio il runlevel 3 (Modo multiutente completo con rete). A questo punto YaST vi permette di impostare un altro runlevel di default; cfr. la tabelle 12.1 a pagina 300. I servizi e demoni si abilitano o disabilitano in questa tabella che vi offre delle informazioni riguardanti i servizi e demoni disponibili, il loro stato di abilitazione e per quali runlevel sono abilitati. Marcando una riga con un clic del mouse, potete attivare le caselle dei runlevel '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' e 'Arresta', decidete se utilizzare un determinato servizio. Con 'Aggiorna', potete verificare lo stato attuale, nel caso in cui non sia già stato fatto automaticamente. 'Ripristinare valore di default' riporta il sistema allo stato dopo l'installazione. 'Attiva servizio' appare solo se il servizio in questione non è attivo. 'Riportare tutti i servizi al valore default' ripristina lo stato dei servizi così come erano 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

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 con la nuova release è diventato ormai obsoleto. Quando installate SuSE Linux questo file non viene più creato. La configurazione del sistema si realizza adesso tramite i file che si trovano sotto `/etc/sysconfig`. Se eseguite un aggiornamento ed vi è già `/etc/rc.config` sul vostro sistema, il file chiaramente non verrà cancellato.

I file di `/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, dovete in seguito anche lanciare SuSEconfig, per assicurare che le nuove impostazioni vengano applicate. Se usate l'editor sysconfig di YaST2, 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:

  ```
  terra:~ #  init 1
  ```

- Modificate i file di configurazione. Servitevi a riguardo di un editor di testo o, meglio, dell'editor Sysconfig di YaST2; cfr. la sezione *L'editor sysconfig di YaST2* nella pagina successiva.

  Nota

  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 (per 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.

  Nota

- 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 (nell'esempio, 3) con:

```
terra:~ #  init 3
```

Questa procedura si rende chiaramente necessaria solo nel caso di modifiche di ampia portata (ad esempio, la configurazione di rete). In casi più semplici non è neanche necessario che l'amministratore passi al "modo utente singolo"; tuttavia, assicuratevi che tutti i programmi interessati dalle modifiche apportate vengano riavviati.

Suggerimento

Potete disattivare la configurazione automatica tramite SuSEconfig *globalmente* impostando la variabile ⟨*ENABLE_SUSECONFIG*⟩ in `/etc/sysconfig/suseconfig` su `no`. Per poter usufruire del supporto all'installazione, la variabile ⟨*ENABLE_SUSECONFIG*⟩ dovrà tuttavia essere impostata su `yes`. Potete disattivare in modo mirato anche solo determinate sezioni della configurazione automatica.

Suggerimento

L'editor sysconfig di YaST2

Nella directory `/etc/sysconfig`, troverete tutti i file contenenti le impostazioni principali per SuSE Linux. L'editor sysconfig di YaST2 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 che trovate sotto `/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 la funzionalità del vostro sistema. Tutta una serie di variabili sysconfig dei file sotto `/etc/sysconfig/` sono accompagnate da commenti che illustrano la funzione della variabile in questione.

Attenzione

L'editor sysconfig di YaST è composto da tre parti. 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 il lancio di determinati servizi e script qualora lo riteneste opportuno.

Parte IV

Rete

13

Fondamenti del collegamento in 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 normalmente usato 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.

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 militari e, nella forma usata oggi, è stato definito circa nel 1981 in un cosiddetto RFC (ingl. *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.

Suggerimento

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`

Suggerimento

I servizi nominati nella tabella 13.1 a fronte, sono disponibili per scambiare dei dati fra due computer Linux tramite TCP/IP:

Protocollo	Descrizione
TCP	(ingl. *Transmission control protocol*) Protocollo orientato alla connessione. Dal punto di vista dell'applicazione, i dati da trasmettere vengono inviati come 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 allo stesso modo in cui sono stati spediti. TCP assicura che non vadano persi dei dati per strada, e che non vengano mescolati. TCP viene usato dove è saliente la sequenza dei dati.
UDP	(ingl. *User Datagram protocol*) Un protocollo non orientato alla connessione: i dati vengono spediti in pacchetti, e i pacchetti di dati vengono generati dall'applicazione. Non è garantita la sequenza dei dati che giunge a destinazione, e può verificarsi la perdità di singoli pacchetti. UDP è adatto per applicazioni orientati al set di dati, e ha una latenza inferiore al TCP.

Tabella 13.1: *Continua alla pagina seguente...*

ICMP	(ingl. *Internet control message protocol*) Fondamentalmente, questo non è un protocollo per utenti, ma uno speciale protocollo di controllo che trasmette comunicazioni di errori, ed è in grado di verificare il comportamento dei computer interessati alla trasmissione di dati con TCP/IP. Inoltre, con ICMP, viene messo a disposizione anche uno speciale "modo echo" che può venire esaminato con il programma ping.
IGMP	(ingl. *Internet group management protocol*) Questo protocollo regola il comportamento dei computer che usano il multicast IP. Purtroppo, in questo ambito, non possiamo presentarvi il multicasting IP.

Tabella 13.1: *Diversi protocolli del gruppo di protocolli TCP/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.

Modello a strati

Tramite IP (ingl. *Internet protocol*) si ha una trasmissione di dati non garantita. TCP (ingl. *Transmission control protocol*) è in un certo senso un "sopralzo" del sottostante IP, per garantire una trasmissione garantita dei dati. IP a sua volta è 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 13.1 nella pagina successiva.

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, si 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.

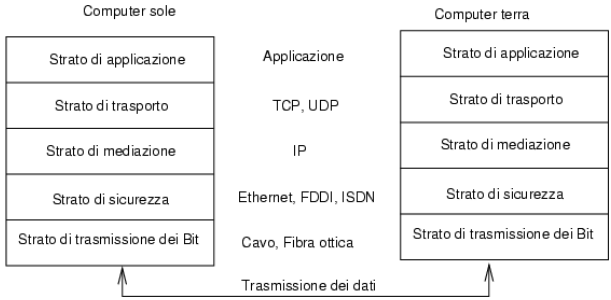


Figura 13.1: *Modello a strati semplificato per TCP/IP*

- Mentre lo strato 1 si occupa del tipo di cavi, delle forme dei segnali, del codice dei segnali e di cose simili, lo strato 2 è responsabile per il procedimento di accesso (quale computer può inviare dati e quando?) e la correzione degli errori (sicurezza dei dati, perciò *strato di sicurezza*). Lo strato 1 viene nominato *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 allo 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 compostoe come rappresentato nella figura 13.2 a fronte.

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

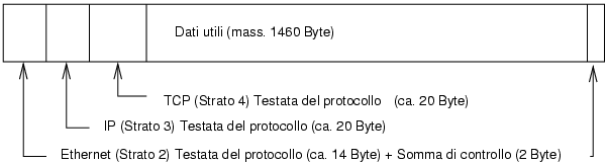


Figura 13.2: *Pacchetto TCP/IP nell'Ethernet*

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.

Indirizzi IP e routing

Nota

Nei seguenti paragrafi diamo una descrizione di reti IPv4. Per avere delle informazioni riguardanti la versione successiva IPv6 del protocollo consulatate la sezione *IPv6 – l'Internet di prossima generazione* a pagina 322.

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 13.2 nella pagina seguente:

Indirizzo IP (binario):	11000000	10101000	00000000	00010100
Indirizzo IP (decimale):	192.	168.	0.	20

Tabella 13.2: *Sintassi di un indirizzo IP*

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 non ci riguardano 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 sono stati assegnati più o meno casualmente, e quindi inutili per contattare un host remoto. L'indirizzo *MAC* occupa però un ruolo molto importante 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 (ingl. *classless inter domain routing*)).

Maschere di rete e routing

Poiché, in un primo tempo, il computer con l'indirizzo IP `192.168.0.20` non può sapere dove si trova il computer con l'indirizzo `192.168.0.1`, 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

Indirizzo IP:192.168.0.20	11000000	10101000	00000000	00010100
Maschera 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 rete: 255.255.255.0	11111111	11111111	11111111	00000000
Risultato binario	11010101	10111111	00001111	00000000
Risultato decimale	213.	95.	15.	0

Tabella 13.3: *Collegamento degli indirizzi IP con la maschera rete*

collegato bit dopor bit con la maschera di rete tramite l'operatore logico AND (vd. tabella 13.3). Di regola, se sono disponibili più interfacce di rete, vengono controllati tutti i possibili indirizzi del mittente.

I risultati dei collegamenti AND vengono confrontati. Se i risultati sono esattamente concordanti, significa che il computer meta si trova nella stessa sottorete, in caso contrario deve venire 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 13.3.

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 dopo 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 *n*ella 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 del prezzo, 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 il 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 ogni altro computer, finchè il pacchetto raggiunge la sua destinazione o scade la TTL (ingl. *time to live*) del pacchetto.

Tipo di indirizzo	Descrizione
L'indirizzo di 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 13.3 nella pagina precedente sotto Risultato. Questo indirizzo non può venire assegnato a nessun 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 al proprio computer.

Tabella 13.4: *Indirizzi speciali*

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 in RFC 1597:

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

Tabella 13.5: *Aree indirizzi IP privati*

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, per esempio `laurent.suse.de` scritto nel formato `hostname.dominio`. Un nome completo (in gergo "Fully qualified domain name" o *FQDN*) si compone del 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 (per esempio `.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

con competenza per un determinato top level domain. Nel caso del top level domain italiano it l'IT-NIC ad avere la competenza per i 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 *DNS – Domain Name System* a pagina 344.

whois

Il protocollo whois è strettamente "imparentato" con DNS. Con l'omonimo programma whois, potrete scoprire velocemente quale server è quello responsabile per un determinato dominio.

IPv6 – l'Internet di prossima generazione

Negli ultimi 10 anni, come conseguenza del boom del (ingl. *World Wide Web*), l'Internet, e con esso i computer che "parlano" il linguaggio TCP/IP, sono aumentati 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 cresciuto da poche migliaia a ca. 100 milioni.

Come sapete, un indirizzo IP è formato "solo" da 32 bit. Alcuni indirizzi IP rimangono inutilizzati per motivi che illustreremo. Come saprete, l'Internet è suddiviso in sottoreti, cioè in rete parziali che si compongono di un valore allo 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 solo 254 sono utilizzabili. 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 (ingl. *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 manutenere. 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, indirizzo gateway ed eventualmente un server dei nomi. Tutte queste informazioni le dovete "conoscere" senza che vi sia la possibilità 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.

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 *L'indirizzo di IPv6* nella pagina successiva.

Ulteriori vantaggi del nuovo protocollo in rassegna:

Configurazione automatica IPv6 ricorre al 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 meccanismo di configurazione automatica del terminale il proprio indirizzo viene dedotto dalle informazioni che giungono dal "Neighbor Discovery Protocol" (ND) dei 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 che non bisogna 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 ad un tratto si passi 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 sogtunnel (vedi la sezione *IPv4 versus IPv6* a pagina 329). 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 (per esempio 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 per esempio "tutti i server dei nomi" (ingl. *all nameservers multicast group*), oppure "tutti i router" (ingl. *all routers multicast group*).

L'indirizzo di 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 una estensione dello spazio di indirizzamento a 128 bit; il secondo attraverso una struttura gerarchica degli indirizzi, meccanismi intelligenti per l'allocazione dell'indirizzo di rete e la possibilità del "multi-homing" (diversi indirizzi per ogni interfaccia di rete con accesso a reti diverse).

Per quel che riguarda IPv6 si distinguono i seguenti tre tipi di indirizzo:

unicast Gli indirizzi di questo tipo vengono assegnati ad una determinata interfaccia di rete. I pacchetti dati 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 identificano 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 ricevano 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) espressi nel modo esadezimale. 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 16 vi mostra questo procedimento con tre modi di rappresentare lo stesso indirizzo.

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                            : 10 : 1000 : 1a4
```

output 16: *Esempio di un indirizzo IPv6*

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 rappresenta la parte dell'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 17 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 trovi all'interno o al di fuori di una determinata sottorete.

```
fe80::10:1000:1a4/64
```

output 17: *Indirizzo IPv6 con prefisso*

IPv6 conosce diversi prefissi che hanno un significato ben preciso (vedi la tabella 13.6 nella pagina successiva).

Prefisso (esadecimale)	**Uso**
00	IPv4 ed IPv4 tramite indirizzi di compatibilità IPv6. Si tratta di un indirizzo compatibile con IPv4. Un router adatto converte 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*), `2002::/16` (*6to4 address space*) e `3ffe::/16` (*6bone.net*).
`fe80::/10`	Indirizzi (ingl. *link-local*) con questo prefisso non vengono instradati (routed), e perciò si muovono solo all'interno della stessa sottorete.
`fec0::/10`	(ingl. *site-local*) Questi indirizzi possono venire instradati (routed), ma solo all'interno di una organizzazione. Così, questi indirizzi sono paragonabili alle reti "private" (p.e. `10.x.x.x`).

Tabella 13.6: *Continua alla pagina seguente...*

ff	Indirizzi IPv6 (ingl. *multicast*) che iniziano con ff sono indirizzi multicast.

Tabella 13.6: *Diversi prefissi IPv6*

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 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 a livello mondiale 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 prelevati 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 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 13 a pagina 329). 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 tipi di indirizzo può essere utilizzato solamente nella sottorete locale. I router non inoltrano dei pacchetti con un indirizzo di destinazinone 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 vogliono indicare 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 sulle 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 "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 in cui si trova l'host.

Se un terminale è presente una volta in una rete ed una volta in un'altra, 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 nelle reti 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 è presente. 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.

IPv4 versus IPv6

Il passaggio da IPv4 a IPv6 di tutti i computer presenti su Internet richiederà del tempo, 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 *Struttura di un indirizzo IPv6* a pagina 325) sono i metodi che permettono di affrontare questa questione.

Le meno diffuse reti IPv6 realizzano lo scambio di dati in reti IPv4, che al momento sono quelli dominanti, 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 (ingl. *Local Area Network*) immensa. In tal maniera viene determinata in modo automatico l'estremita 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 per il mondo 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

In mezzo all'Internet già un pò "fuori moda" con *6Bone* (www.6bone.net) si ha 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

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 libri:

`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 1725 L'RFC introduttivo al tema IPv6.

IPv6 Essentials In inglese. Hagen, Silvia: *IPv6 Essentials*. O'Reilly & Associates, 2002. - (ISBN 0-596-00125-8).

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, p.e., 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`. Le modifiche nella configurazione di rete a partire da SuSE Linux 8.0 sono documentati nel file: `/usr/share/doc/packages/sysconfig/README`.

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 automaticamente integrato. Potete vedere se la scheda è stata integrata correttamente dall'output del comando `ifstatus eth0` che indica il device 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 per esempio in questo modo: `alias eth0 tulip`. Ciò avviene automaticamente, se in linuxrc, durante la prima installazione, viene caricato il supporto dell'unità di disco per la scheda di rete. Successivamente, questo compito può venire svolto con YaST.

Con schede di rete hotplug (per esempio PCMCIA o USB) i driver vengono rilevati automaticamente al momento del loro inserimento; non bisogna configurare alcunché, per ulteriori dettagli consultate il capitolo *Hotplug* a pagina 207.

Configurazione con YaST

La scheda di rete si lascia configurare in pochi minuti con YaST . Selezionate nel Centro di controllo 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 menù della configurazione dei dati dell'hardware della scheda rete. Il menu è rappresentato nella figura 13.3.

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 della rete non viene riconosciuto automaticamente. In questo caso, selezionate il punto 'Aggiungi' affinchè possa venir scelto un nuovo modulo del driver.

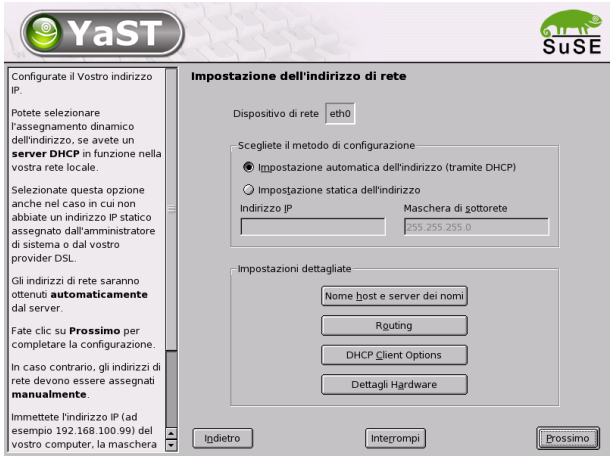


Figura 13.3: *Configurazione dei parametri dell'hardware*

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 dare anche speciali parametri come p.e. l'interfaccia da usare, o se p.e. volete utilizzare sulla scheda il collegamento RJ-45 o BNC. Consultate a proposito la documentazione del modulo driver Per PCMCIA e USB basta attivare la relativa casella.

Dopo l'inserzione dei parametri dell'hardware, potete configurare gli altri dati dell'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 create una rete individuale, potete

orientarvi, per l'attribuzione degli indirizzi, al paragrafo 13 a pagina 314 o alla tabella 13.5 a pagina 321. Altrimenti, immettete nei campi previsti, gli indirizzi assegnati dal vostro amministratore di rete.

Affinché la risoluzione dei nomi funzioni come descritto nel capitolo 13 a pagina 344, non dimenticate di impostare un server dei nomi. Con il punto 'Routing' potete impostare il routing. Per eseguire impostazioni avanzate, selezionate il punto 'Configurazione per esperti'.

Se utilizzate schede di rede radio, attivate la casella 'Wireless Device'. Le principali impostazioni si possono conseguire in un dialogo a parte. Si tratta in particolare del modo di funzionamento, nome della rete e una chiave per la trasmissione di dati cifrata.

La configurazione della rete è a questo punto conclusa. YaST infine lancia SuSEconfig ed immettete le vostre indicazioni nei relativi file. Affinché le impostazioni vengono applicate, dovete riconfigurare i programmi interessati, e riavviare i rispettivi demoni immettendo:

```
terra:~ #  rcnetwork restart
```

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.

Configurare IPv6

Se volete configurare l'IPv6, normalmente, non dovete effettuare alcuna configurazione sulle postazioni di lavoro. È però necessario caricare il supporto per IPv6; potete farlo con il comando

```
terra:~ #  modprobe ipv6
```

Grazie alla filosofia della configurazione automatica di IPv6, viene attribuito alla scheda di rete, un indirizzo nella rete link-local.

Normalmente, su una workstation, non viene amministrata alcuna tabella di routing. La workstation chiede ai router presenti nella rete, con l'aiuto del Router advertisment protocol, quali siano il prefisso e i gateway da usare. Per configurare un router IPv6, potete utilizzare il programma radvd dal pacchetto `radvd`. Questo programma comunica alla workstation, il prefisso da usare per gli indirizzi IPv6 e il/i router.

Per poter assegnare comodamente un indirizzo IPv6 ad una workstation, è quindi consigliabile installare e configurare un router con il programma radvd. In questo modo, le workstation ricevono automaticamente gli indirizzi IPv6.

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 essere assegnata anche all'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 *File di configurazione* nella pagina successiva.

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 possibilmente si adatta quanto 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 secondo l'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-<numerocorrente>`. 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.

File di configurazione

Questo paragrafo riassume i file di configurazione di rete e spiega la loro funzione e 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` ottiene all'occorrenza oltre al nome di interfaccia anche una precisa descrizione di hardware, e poi cerca 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"). La maschera di rete può già contenere l'indirizzo IP (IPADDR="10.10.11.214/16") o si può indicarlo separatamente (NETMASK="255.255.0.0"). La pagina di manuale di `ifup` (`man 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 generale debba venire utilizzata solo per un'interfaccia. Con le variabili `POST_UP_SCRIPT` e `PRE_DOWN_SCRIPT` possono essere eseguiti singoli script dopo l'avvio o prima dell'arresto della 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 trovate le impostazioni generali per DHCP e schede di rete radio. Tutte le variabili da 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 il computer (parola chiave search) e quale sia l'indirizzo del server dei nomi (parola chiave nameserver) che deve venire indirizzato. Può venire indicati più di un nome di dominio. Al momento della risoluzione di un nome non del tutto chiaro si cerca, "attaccando" le singole registrazioni in search, di creare un nome valido e completamente qualificato. Diversi server dei nomi possono venir resi noti tramite più righe inizianti con nameserver. I commenti vengono introdotti da `'#'`.

Il file 33 indica un esempio per `/etc/resolv.conf`.

```
# Il nostro dominio
search cosmo.com
#
# Usiamo sole (192.168.0.1) come server dei nomi
nameserver 192.168.0.1
```

file 33: `/etc/resolv.conf`

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 la permanenza di eventuali versioni modificate di `resolv.conf` (p.e., 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`: in questo caso, lasciar modificare il file resolv.conf a YaST o modificarlo manualmente non fa differenza. In entrambi i casi, si tratta di una modifica mirata e duratura, mentre le modifiche dei servizi menzionati è di natura puramente temporanea.

`/etc/hosts`

In questo file (vd. file 34) vengono assegnati gli indirizzi IP ai computer. Se non si utilizzano server dei nomi, devono venire elencati tutti i computer con i quali deve venire creato un collegamento-IP. Per ogni computer, in questo file viene annotata una riga consistente dell' indirizzo-IP, nome ufficiale e nome del computer (per esempio `terra`). L'indirizzo--IP deve trovarsi all'inizio della riga, le registrazioni vengono separate da spazi o da tabulazioni. I commenti vengono preceduti da `'#'`.

```
127.0.0.1 localhost
192.168.0.1 sole.cosmo.com sole
192.168.0.20 terra.cosmo.com terra
```

file 34: `/etc/hosts`

`/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 35).

```
loopback      127.0.0.0
localnet      192.168.0.0
```

file 35: `/etc/networks`

`/etc/host.conf`

La risoluzione dei nomi, cioè la traduzione di nomi di computer o di reti tramite la libreria *resolver* viene controllata da questo file; questo file viene usato solo per programmi che hanno un link 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 13.7 mostra i parametri possibili.

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 computer registrato in `/etc/hosts` possa avere più indirizzi IP.
nospoof *on* alert *on*/*off*	Questi parametri influenzano lo *spoofing* nel server dei nomi, ma non influiscono sulla configurazione della rete.
trim ⟨*nome di dominio*⟩	Il nome del dominio indicato viene tagliato dal computer prima che questi risolva il nome del computer (sempre che il nome del computer 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.

Tabella 13.7: *Parametri per /etc/host.conf*

Un esempio per `/etc/host.conf` mostra il file 36.

```
# We have named running
order hosts bind
# Allow multiple addrs
multi on
```

file 36: `/etc/host.conf`

`/etc/nsswitch.conf`

Con la GNU C Library 2.0 è arrivato anche il "Name Service Switch" (NSS) (vedi la pagina di manuale di `nsswitch.conf` (`man 5 nsswitch.conf`), come pure più dettagliatamente *The GNU C Library Reference Manual*, capitolo "System Databases and Name Service Switch"; vd. il pacchetto `libcinfo`doc.).

Nel file `/etc/nsswitch.conf` viene stabilito in quale successione verranno richieste determinate informazioni. Un esempio per `nsswitch.conf` viene mostrato nel file 37. I commenti vengono introdotti da `'#'`. Lì per esempio, la registrazione nella "banca dati" `hosts` significa che tramite DNS (cfr. sezione 13 a pagina 344) viene inviata una richiesta a `/etc/hosts` (`files`).

```
passwd:     compat
group:      compat

hosts:      files dns
networks:   files dns

services:   db files
protocols:  db files

netgroup:   files
automount:  files nis
```

file 37: `/etc/nsswitch.conf`

Le "banche dati" disponibili tramite NSS sono indicate nella tabella 13.8 nella pagina successiva; in futuro ci saranno anche `automount`, `bootparams`, `netmasks` e `publickey`.

`aliases`	Alias di mail, usato da `sendmail`(8); vedi la pagina di manuale di `aliases` (`man 5 aliases`).
`ethers`	Indirizzi Ethernet.
`group`	Usato da `getgrent`(3) per gruppi di utenti; vedi la pagina di manuale di `group` (`man 5 group`).
`hosts`	Usato da `gethostbyname`(3) e funzioni simili, per i nomi degli host e indirizzi IP.
`netgroup`	Elenco, nella rete, di host e utenti per regolare i diritti d'accesso; vedi la pagina di manuale di `netgroup` (`man 5 netgroup`).
`networks`	Nomi e indirizzi della rete usati da `getnetent`(3)
`passwd`	Password degli utenti usate da `getpwent`(3); vedi la pagina di manuale di `passwd` (`man 5 passwd`).
`protocols`	Protocolli di rete usati da `getprotoent`(3); vedi la pagina di manuale di `protocols` (`man 5 protocols`).
`rpc`	Nomi e indirizzi "Remote Procedure Call" usati da `getrpcbyname`(3) e da simili funzioni.
`services`	Servizi di rete usati da `getservent`(3).
`shadow`	Password "shadow" degli utenti usate da `getspnam`(3); vedi la pagina di manuale di `shadow` (`man 5 shadow`).

Tabella 13.8: *Banche dati disponibili tramite* `/etc/nsswitch.conf`

Le possibilità di configurazione delle "banche dati" NSS, si trovano nella tabella 13.9 a fronte.

`files`	Accesso diretto ai file, per esempio su `/etc/aliases`.
`db`	Accesso tramite una banca dati.
`nis`	Vedi sezione 13 a pagina 380.
`nisplus`	
`dns`	Da usare come estensione solo con `hosts` e `networks`.
`compat`	Da usare come estensione solo con `passwd`, `shadow` e `group`

Tabella 13.9: *Continua alla pagina seguente...*

inoltre	con determinati risultati di ricerca è possibile provocare reazioni differenti; i dettagli a riguardo si trovano nella pagina di manuale di `nsswitch.conf` (`man 5 nsswitch.conf`).

Tabella 13.9: *Possibilità di configurazione delle banche dati NSS*

`/etc/nscd.conf`

Tramite questo file viene configurato l'nscd (ingl. *Name Service Cache Daemon*); vedi la pagina di manuale di `nscd` (`man 8 nscd`) e la pagina di manuale di `nscd.conf` (`man 5 nscd.conf`). Contiene le informazioni di `passwd`, `groups` e `hosts`. `hosts` non viene letto in modo che non bisogna riavviare il demone se p.es. la risoluzione dei nomi (DNS) viene modificata tramite `/etc/resolv.conf`;

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

```
terra:~ #  rcnscd restart
```

`/etc/HOSTNAME`

Qui si trova il nome del computer, 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 del computer!

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 13.10 nella pagina seguente).

`/etc/init.d/network`	Questo script si occupa della configurazione dell'hardware e del software di rete durante la fase di avvio del sistema.

Tabella 13.10: *Continua alla pagina seguente...*

`/etc/init.d/inetd`	Lancia l'inetd nel caso che sia impostato in `/etc/rc.config`; ciò è necessario se per esempio si vuole eseguire il login su questo computer dalla rete.
`/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/sendmail`	Controlla il processo sendmail.
`/etc/init.d/ypserv`	Lancia il server NIS.
`/etc/init.d/ypbind`	Lancia il client NIS.

Tabella 13.10: *Alcuni script di inizializzazione dei programmi di rete*

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.

Per tutte le interfacce che necessitano un routing particolare, ciò si lascia definire in 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: qui può trovarsi l'indirizzo IP del computer o della rete o, con server dei nomi *raggiungibili*, anche il nome completo, qualificato del computer o di una rete.

- La seconda colonna contiene o il gateway di default o un gateway dietro cui sono raggiungibili o un computer o una rete.
- La terza colonna contiene la maschera di rete per reti o computer dietro un gateway. Per computer dietro un gateway, la maschera è per esempio `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.

DNS – Domain Name System

Compito del DNS (ingl. *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 trovate nella sezione 13 a pagina 321.

I seguenti esempi di configurazione si riferiscono a BIND 9, che adesso rappresenta lo standard in SuSE Linux.

Inizializzare il server 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 e registrate 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 dura un pò. Per ottenere una risoluzione del nome sicura ed effettiva, registrate 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 38 sono stati scelti a caso, dovrete adattatarli in base ai vostri dati effettivi.

```
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;
        };
```

file 38: *Opzioni di forwarding in* `named.conf`

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`.

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 39 vi mostra un esempio di un `/etc/named.conf` ridotto all'osso.

```
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";
};
```

file 39: *File minimale* `/etc/named.conf`

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 il port standard.

Omettendo completamente questa registrazione, vengono usate come standard tutte le interfacce.

query-source address * port 53; questa registrazione può essere necessaria, se un firewall blocca le richieste DNS esterne. In questo modo si induce BIND a inviare richieste all'esterno dal port 53 e non da porte superiori a 1024).

query-source-v6 address * port 53; questa registrazione va 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 chiunque

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 alcune sono state rimosse. 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.

La sezione di configurazione logging

BIND permette di configurare in modo flessibile l'attività di logging. Normalmente, le preimpostazioni dovrebbero rilevarsi sufficienti. L'esempio 40 vi mostra la variante più semplice di una tale registrazione, e sopprime completamente il "logging":

```
logging {
        category default { null; };
};
```

file 40: *Il logging viene soppresso*

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 41.

```
zone "mio-dominio.it" in {
       type master;
       file "mio-dominio.zone";
       notify no;
};
```

file 41: *L'indicazione zone per mio-dominio.it*

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 42.

```
zone "altro-dominio.it" in {
        type slave;
        file "slave/altro-dominio.zone";
        masters { 10.0.0.1; };
};
```

file 42: *L'indicazione zone per altro-dominio.it*

Le opzioni di zone:

type master; `master` stabilisce che *questa* zona venga amministrata su *questo* name server. 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 è 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.

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. È 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 `mondo.all`; cfr. il file 43.

```
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
```

file 43: File `/var/lib/named/mondo.zone`

Riga 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'.

Riga 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.

Riga 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 ed da un numero progressivo, nella forma AAAAMMGGNN.

Riga 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).

Riga 5: Il retry rate indica l'intervallo di tempo trascorso il quale un name server secondario cerca di ristabilire il contatto con il server primario, in caso di errore. In questo caso, due ore (2H = 2 hours).

Riga 6: L'expiration time indica quanto tempo debba passare prima che il server dei nomi secondario espelli i dati nella cache, se non riesce a ristabilire il contatto con il server primario. In questo caso, una settimana (1W = 1 week).

Riga 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, qualora non possano essere risolte.

Riga 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, verrano informati tutti i server dei nomi qui elencati delle modifiche apportate ai dati delle zone.

Riga 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, 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.

Riga 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;cfr. 44.

```
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.
```

file 44: *Risoluzione inversa dell'indirizzo*

Riga 1: $TTL definisce il TTL di default valido per tutte le voci.

Riga 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.

Riga 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.

Riga 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 '.'. 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.

Transazioni sicure

Grazie alle "Transaction SIGnatures" (TSIG) si realizza una transazione sicura. Vengono utilizzate delle chiavi di transazione (ingl. *transaction keys*) e firme di

transazione (ingl. *transaction signatures*). Nella seguente sezione spiegheremo come generarle ed utilizzarle.

Una transazione sicura è richiesta per la comunicazione tra server e l'aggiornamento dinamico dei dati di zona. Il controllo degli accessi basato su chiave offre maggior sicurezza rispetto ad un controllo basato sugli indirizzi IP.

Con il seguente comando potete generare una chiave di transazione (per avere ulteriori informazioni vedi la pagina di manuale di `dnssec-keygen` (`man dnssec-keygen`)):

```
dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2.
```

Il risultato sono due file che per esempio portano il seguente nome:

```
Khost1-host2.+157+34265.private
Khost1-host2.+157+34265.key
```

La chiave è contenuta in entrambi i file (p.e. `ejIkuCyyGJwwuN3xAteKgg==`). In seguito `Khost1-host2.+157+34265.key` dovrebbe venir copiato in modo sicuro (per esempio 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` sul server il file `/etc/named.conf` 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 la parte intitolata update-policy.

Aggiornamento dinamico dei dati di zona

Con aggiornamento dinamico (ingl. *dynamic update*) si intende l'aggiunta, la modifica e l'eliminazione di registrazioni nei dati zona di un master. Questo meccanismo viene descritto nell'RFC 2136.

L'aggiornamento dinamico delle zone si configura tramite le opzioni allow-update o update-policy nelle registrazioni delle zone. Le zone che vengono aggiornate dinamicamente non dovrebbero venir impostate manualmente.

Con `nsupdate` le registrazioni da aggiornare vengono trasmesse al server; per la corretta sintassi vedi la pagina di manuale di `nsupdate` (`man 8 nsupdate`). L'aggiornamento deve avvenire assolutamente, per motivi di sicurezza, per via di transazioni sicure (TSIG); cfr. la sezione 13 a pagina 352.

DNSSEC

DNSSEC (ingl. *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 (ingl. *public keys*) dovrebbero essere integrate nei file zona con $INCLUDE.

Tutte le chiavi possono essere riuniti in un set di chiavi tramite `dnssec-makekeyset` da trasmettere in modo sicuro alla zona superiore (ingl. *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.

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.

LDAP – Un servizio directory

In ambienti di lavoro collegati in rete è determinante che le informazioni importanti siano tenuti in serbo in modo strutturato e siano immediatamente disponibili. 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 di tutti i giorni, contiene le informazioni richieste in una forma ben strutturata, di facile consultazione ed immediatamente individuabili.

Nel caso ideale vi è un server centrale contenente i dati in una determinata directory che li distribuisce ai client nella rete tramite un protocollo particolare. I dati dovrebbero essere strutturati in modo che una gamma quanto vasta possibile di applicativi possa accedervi. In tal modo non ogni tool per calendari o e-mail client deve avere una propria banca dati, ma potrebbe accedere ad uno stock di dati mantenuti centralmente. Questo ridurrebbe notevolmente gli interventi di amministrazione per le informazioni in questione. Un protocollo aperto e standardizzato come LDAP assicura che un numero quanto vasto 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 di solito con un servizio directory si amministrano dati possibilmente *statici*, mentre i dati di una banca dati convenzionale sono di solito *dinamici* 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 che assume 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 nella loro insieme. Banche dati supportano queste transazioni, directory no. Nel caso delle directory 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. Novells NDS, Microsofts ADS, Banyans Street Talk e lo standard OSI X.500.

Originariamente LDAP è stato concepito come versione 'snella' di DAP (ingl. *Directory Access Protocol*), sviluppato per l'accesso a X.500. Lo standard X.500 regola la disposizione gerarchica delle voci della directory.

LDAP è stato '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 distribuite. 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 progettato all'inizio. Con slapd esiste un server Open Source con il quale potete archiviare i dati degli oggetti in una banca dati locale. Questo server viene completato da slurpd responsabile per la replica di più server LDAP.

Il pacchetto openldap2 è composto principalmente da due programmi.

slapd Un server LDAPv3 stand-alone che amministra i dati degli oggetti in un database basato su BerkeleyDB.

slurpd Questo programma replica le modifiche apportate ai dati del server LDAP locale agli altri server LDAP presenti nella rete.

Tools aggiuntivi `slapcat`, `slapadd`, `slapindex`

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. Il server centrale, tramite i client, distribuisce nella rete i dati di configurazione dei file `/etc` e directory `group`, `hosts`, `mail`, `netgroup`, `networks`, `passwd`, `printcap`, `protocols`, `rpc` e `services`. L'amministrazione di questi semplici file di testo risulta essere semplice, ma il tutto diventa più complicato quando si tratta di gestire una maggior quantitativo di dati, visto che manca ogni tipo di strutturazione. NIS è stato ideato solo per piattaforme Unix, quindi non può essere utilizzato per l'amministrazione centralizzata dei dati in una rete eterogenea.

LDAP invece non si limita a reti puramente Unix. Server Windows (a partire da Windows 2000) supportano LDAP quale servizio di directory. Anche Novell offre il servizio LDAP. Inoltre, LDAP sa fare più di quanto riferito finora.

LDAP può essere utilizzato per qualisiasi struttura di dati da amministrare centralmente. Ecco alcuni esempi:

- sostituire un server NIS
- mail routing (postfix, sendmail)
- rubriche per mail client come Mozilla, Evolution, Outlook, ...
- gestire 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.

Struttura dell'albero directory di LDAP

Una directory LDAP ha una struttura ad albero. Tutte le registrazioni (chiamati 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` (ingl. *country*), `dc` (ingl. *domainComponent*) oppure `o` (ingl. *organization*).

La relazione nella quale si trovano tra di loro i singoli elementi di un albero di directory LDAP viene illustrata nel seguente esempio (vedi figura 13.4).

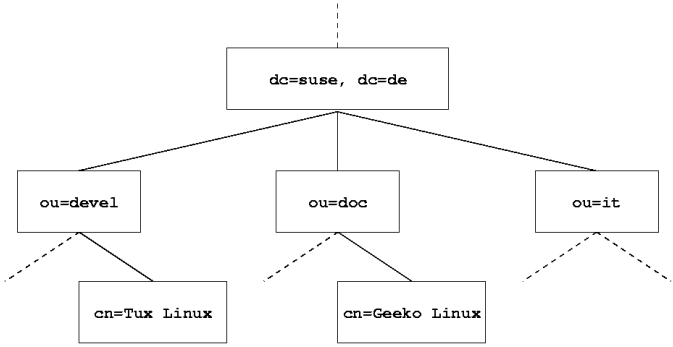


Figura 13.4: *Struttura di una directory LDAP*

L'intera figura comprende un *Directory Information Tree* esempio. Vedete le registrazioni (ingl. *entries*) 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 debbano essere archiviati 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 13.11 nella pagina successiva offre una rassegna delle classi di oggetto utilizzate nell'esempio presi da `core.schema` e `inetorgperson.schema` con gli attributi necessari e valori di attributo adatti.

Classe di oggetto	Significato	Registrazione esempio	Attributi necessari
dcObject	*domainComponent* (componenti del nome di dominio)	suse	dc
organizationalUnit	*organizationalUnit* (unità d'organizzazione)	doc	ou
inetOrgPerson	*inetOrgPerson* (dati relativi ad una persona per Intranet/Internet)	Geeko Linux	sn e cn

Tabella 13.11: *Classi di oggetto e attributi ricorrenti*

Nell'output 18 vedete un'estratto esemplare di una direttiva schema con commenti che vi aiuteranno a comprendere la sintassi di nuovi schemi.

```
...
#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) )
...
```

output 18: *Estratto dal schema.core*
(A scopo esplicativo sono state numerate le righe)

Come esempio abbiamo il tipo di attributo `organizationalUnitName` e la classe di oggetto relativa `organizationalUnit`. Nella prima riga abbiamo il nome dell'attributo, OID (*Object Identifier*) (numerico) univoco e l'abbreviazione

dell'attributo. La riga 2 viene introdotta da `DESC`, una breve descrizione dell'attributo a cui qui segue l'indicazione del relativo RFC a cui risale la definizione. `SUP` nella riga 3 rimanda ad un tipo di attributo superiore, a cui appartiene questo attributo.

La definizione della classe di oggetto `organizationalUnit` inizia alla riga 4 come per la definizione dell'attributo con un OID ed un nome per la classe di oggetto. Nella riga 5 abbiamo una breve descrizione della classe di oggetto. Con la registrazione `SUP top` la riga 6 vi indica che questa classe di oggetto non è subordinata ad un'altra classe di oggetto. Nella riga 7 vengono indicati dopo `MUST` tutti i tipi di attributo che*devono* essere utilizzati in un oggetto del tipo `organizationalUnit`. Nella riga 8, dopo `MAY` avete l'elenco dei tipi di attributo che *possono* essere utilizzati con questa classi di oggetti.

Per una introduzione molto valida per quel che riguarda l'uso degli schemi rimandiamo alla documentazione su OpenLDAP che trovate nel vostro sistema installato sotto `/usr/share/doc/packages/openldap2/admin-guide/index.html`.

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

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/inetorgperson.schema
```

output 19: *slapd.conf: direttiva include per schemi*

Con questa prima direttiva in `slapd.conf` viene specificato lo schema secondo il quale è organizzata la vostra directory LDAP (vedi l'output 19).
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.

```
pidfile /var/run/slapd.pid
argsfile /var/run/slapd.args
```

output 20: *slapd.conf: pidfile ed argsfile*

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.

```
%
%

#
# 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!
```

output 21: *slapd.conf: controllo di accesso*

Nell'output 21 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 linee di orientamento 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 introdotta nel file di configurazione. Quindi le regole di ordine generale dovrebbero seguire a quelle più specifiche. slapd elaborerà la prima regola che giudica 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 tabelle 13.12):

Identificatore	Significato
`*`	tutti gli utenti senza eccezione alcuna
`anonymous`	utenti non autenticati ("anonimi")
`users`	utenti autenticati
`self`	utenti in relazione con l'oggetto target
`dn=<regex>`	tutti gli utenti per i quali vale questa espressione regolare

Tabella 13.12: *Gruppi di utenti con permesso di accesso*

- ⟨*access*⟩ specifica il tipo di accesso. Si distingue tra le possibilità riportate nella tabella 13.13:

Identificatore	Significato
`none`	accesso non consentito
`auth`	per la presa di contatto con il server
`compare`	per l'accesso comparativo su oggetti
`search`	per l'applicazione di filtri di ricerca
`read`	permesso di lettura
`write`	permesso di scrittura

Tabella 13.13: *Tipi di accesso*

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 22 vedete un esempio per un controllo degli accessi semplice su cui potete intervenire a piacimento tramite l'uso di espressioni regolari.

```
acess to dn.regex="ou=([^,]+),dc=suse,dc=de"
      by cn=administrator,ou=$1,dc=suse,dc=de write
      by user read
      by * none
```

output 22: *slapd.conf: esempio di controllo degli accessi*

Questa regola stabilisce che sulle registrazioni `ou` solo il relativo amministratore ha l'accesso in scrittura. Gli altri utenti autenticati hanno il permesso di lettura ed a tutti gli altri viene negato ogni accesso.

Suggerimento

Creare 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.

Suggerimento

Informazioni dettagliate ed una configurazione esempio dei permessi di accesso LDAP sono reperibili nella documentazione in linea del pacchetto installato openldap2.

Oltre alla possibilità di amministrare i controlli di accesso tramite il file di configurazione centrale del server (`slapd.conf`) vi è la possibilità di ricorrere agli ACI (ingl. *Access Control Information*), per mezzo dei quali le informazioni di accesso per i singoli oggetti possono essere archiviati 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

```
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
```

***output* 23:** *slapd.conf: Direttive riguardanti la banca dati*

Nella prima riga di questa sezione (vedi output 23) viene stabilito il tipo di banca dati, nell'esempio LDBM. Tramite `suffix` nella seconda riga 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 per l'amministrazione di 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 *Gestione dei dati nella directory LDAP* nella pagina successiva), 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 *L'editor*

dei runlevel editor di YaST a pagina 305) oppure create i relativi collegamenti dei script di avvio e di arresto sulla riga di comando tramite `insserv` (vedi la sezione *Aggiungere script di inizializzazione* a pagina 303).

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'aggiungere nuovi dati. OpenLDAP utilizza a tal fine il comando `ldapadd`. Per motivi di praticità si consiglia di aggiungere gli oggetti alla banca dati possibilmente in gruppi. A tal fine LDAP supporta il cosiddetto formato LDIF (ingl. *LDAP Data Interchange Format*). Un file LDIF è un semplice file di testo che può contenere un numero qualsiasi di coppie di valori e attributi. Per vedere quali siano le classi di oggetto e attributi disponibili, consultate i file schema indicati in `slapd.conf`. Un semplice file LDIF adatto al nostro esempio (la figura 13.4 a pagina 359) assumerebbe il seguente aspetto (vedi file 45):

```
# L'organizzazione SuSE
dn: dc=suse,dc=de
objectClass: dcObject
objectClass: organization
o: SuSE AG
dc: suse

# L'unità di organizzazione sviluppo (devel)
dn: ou=devel,dc=suse,dc=de
objectClass: organizationalUnit
ou: devel

# L'unità di organizzazione documentazione (doc)
dn: ou=doc,dc=suse,dc=de
objectClass: organizationalUnit
ou: doc

# L'unità di organizzazione reparto IT (it)
```

```
dn: ou=it,dc=suse,dc=de
objectClass: organizationalUnit
ou: it
```

file 45: *Esempio di un file LDIF*

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 consegnatelo 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'output 24 vedete il comando `ldapadd` in dettaglio.

```
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"
```

output 24: *ldapadd di esempio.ldif*

I dati utenti dei singoli addetti possono venir raccolti in file LDIF distinti. Nel seguente esempio `tux.ldif` (vedi output 25) aggiungiamo l'addetto `Tux` alla nuova directory LDAP:

```
# L'addetto Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
objectClass: inetOrgPerson
cn: Tux Linux
givenName: Tux
mail: tux@suse.de
uid: tux
telephoneNumber: +49 1234 567-8
```

output 25: *File LDIF per Tux*

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 `+49 1234 567-8` a `+49 1234 567-10`, editate il file LDIF come mostrato nell' output 26.

```
# L'addetto Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
changetype: modify
replace: telephoneNumber
telephoneNumber: +49 1234 567-10
```

output 26: *File LDIF modificato: tux.ldif*

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: +49 1234 567-10
```

Leggete la pagina di manuale di `ldapmodify` per avere delle informazioni dettagliate su `ldapmodify` e la sua sintassi.

Come ricercare dati nella directory LDAP

OpenLDAP offre con `ldapsearch` un tool per la riga di comando atto a rilevare dei dati nella directory LDAP. Un comando di ricerca semplice presente 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
```

Configurazione LDAP con YaST

Nota

Configurazione del server LDAP

YaST vi assiste nell'organizzare le registrazioni delle directory, non però nella configurazione del server LDAP. Prima di iniziare a lavorare con il modulo di YaST client LDAP, il server LDAP deve già esser stato impostato correttamente (integrazione degli schemi, ACL adatte, comportamento di avvio etc.). Accanto agli schemi tipici di NIS (`cosine.schema` e `rfc2307bis.schema`) all'elenco degli schemi va aggiunto `yast2userconfig.schema`. Inoltre il server LDAP deve disporre di almeno una registrazione base sotto la quale inserire le altre registrazioni. Create questa registrazione come descritto in precedenza con `ldapadd` come file `.ldif`.

Nota

Al posto di NIS, SuSE Linux vi permette di utilizzare LDAP per l'amministrazione dei dati dei gruppi e utenti. YaST vi offre sotto 'Servizi di rete' → 'Client LDAP' un modulo per configurare l'autenticazione dell'utente nella rete. Qui potete abilitare LDAP per l'amministrazione dei dati dell'utente e definire le registrazioni di default da consultare alla creazione di nuovi utenti o gruppi nei corrispondenti moduli YaST.

Processo generale

Per comprendere meglio il funzionamento del modulo LDAP di YaST dovreste conoscere un pò i processi che si svolgono 'dietro le quinte' sul client. Innazitutto, non appena abilitate durante l'installazione LDAP per l'autenticazione di rete oppure lanciate il modulo YaST, vengono installati i pacchetti `pam_ldap` ed `nss_ldap` , e adattati i corrispondenti file di configurazione.

Con `pam_ldap` viene utilizzato il modulo PAM responsabile per la comunicazione tra processi di login e directory LDAP quale fonte dei dati di autenticazione. Viene installato il relativo modulo di software `pam_ldap.so` e adattata la configurazione PAM (vedi output 27).

```
auth:       use_ldap nullok
account:    use_ldap
password:   use_ldap nullok
session:    none
```

output 27: *pam_unix2.conf adatto per LDAP*

Se volete configurare manualmente ulteriori servizi LDAP, il modulo LDAP-PAM deve essere inserito nel file di configurazione PAM corrispondente al servizio che trovate sotto `/etc/pam.d/`. File di configurazione già adattati per dei servizi si trovano sotto `/usr/share/doc/packages/pam_ldap/pam.d/`. Copiate i file corrispondenti sotto `/etc/pam.d/`.

Tramite `nss_ldap` adattate la risoluzione dei nomi di `glibc`, per via del meccanismo `nsswitch`, all'utilizzo di LDAP. Dopo aver installato questo pacchetto sotto `/etc/` troverete un nuovo file adattato `nsswitch.conf`. Per sapere di più sul funzionamento di `nsswitch.conf` andate alla sezione *File di configurazione* a pagina 335. Per l'amministrazione degli utenti ovvero l'autenticazione tramite LDAP, il vostro `nsswitch.conf` deve contenere le seguenti righe (cfr.output 28):

```
passwd: files ldap
group:  files ldap
```

output 28: *Adattamenti in nsswitch.conf*

Queste righe istruiscono la libreria resolver di `glibc`, di analizzare, quale fonte per i dati di autenticazione e dati utenti, innanzitutto i file corrispondenti locali del sistema sotto`/etc` e di accedere inoltre al server LDAP. Provate questo meccanismo facendovi mostrare tramite il comando `getent passwd` il contenuto della banca dati degli utenti. Nell'elenco dovrebbero comparire sia gli utenti locali del vostro sistema che tutti gli utenti del server LDAP.

Moduli e template – configurazione con YaST

Dopo che `nss_ldap` e `pam_ldap` sono stati adattati da YaST potete iniziare nel primo dialogo di YaST con la configurazione vera e propria.

Nota

Utilizzare il client YaST

Il client LDAP di YaST serve ad adattare, ed all'occorrenza ampliare, i moduli di YaST per l'amministrazione di utenti e gruppi. Inoltre potete definire dei template con valori di default per i singoli attributi per semplificare il processo di rilevamento dei dati vero e proprio. I valori impostati qui vengono archiviati automaticamente sotto forma di oggetti LDAP nella directory LDAP. I dati dell'utente vengono immessi nei dialoghi di YaST. Le informazioni inserite vengono archiviate sotto forma di oggetti nella directory LDAP.

Nota

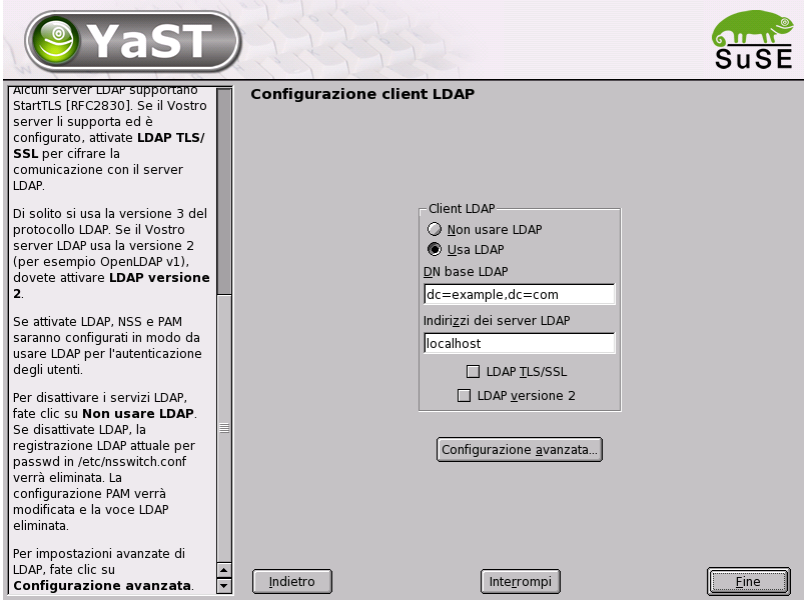


Figura 13.5: *YaST: configurazione del client LDAP*

Nel primo dialogo abilitate attraverso radio bottoni l'utilizzo di LDAP per l'autenticazione degli utenti e sotto 'DN base LDAP' immettete la base di ricerca sul server, al di sotto della quale si trovano tutti i dati sul server LDAP. Nel secondo campo di immissione 'Indirizzo dei server LDAP' immettete l'indirizzo del server LDAP. Se il vostro server supporta StartTLS, marcate la voce 'LDAP TLS/SSL', per consentire una comunicazione cifrata tra client e server. Se come amministratore volete modificare attivamente dei dati sul server, fate clic su 'Configurazione avanzata'.

Per modificare la configurazione del server LDAP immettete nel dialogo i dati di accesso richiesti. Si tratta dei 'DN di base della configurazione', al di sotto dei quali si trovano tutti gli oggetti di configurazione, e 'Bind DN'. Il Bind DN è in questo caso il vostro DN utente.

Attivate la voce 'Server dei file', se il sistema sul quale viene eseguito questo modulo di YaST è il file server della vostra rete.

Per intervenire sulle registrazioni del server LDAP, fate clic su 'Configura le impostazioni archivati su server'. Compare una finestra in cui immettere la password LDAP per autenticarsi sul server. In base alle ACL o ACI del server vi sarà concesso l'accesso ai moduli di configurazione sul server.

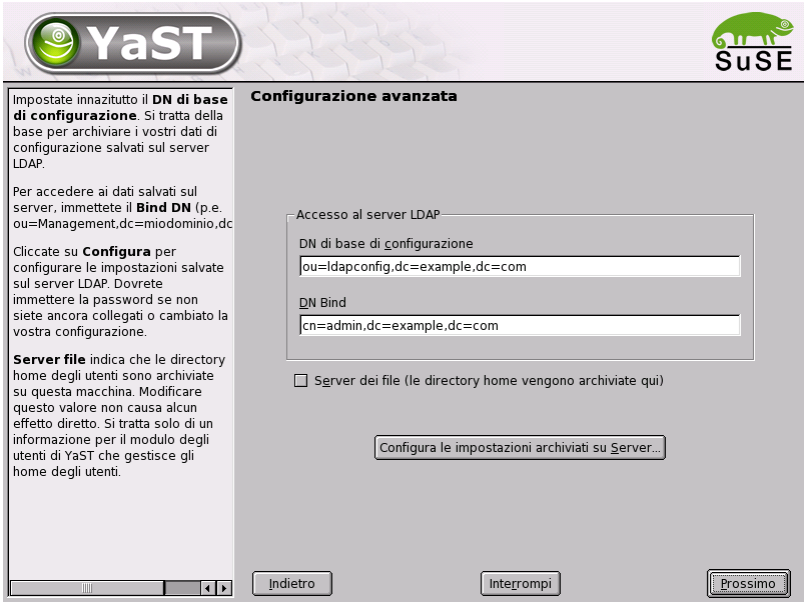


Figura 13.6: *YaST: configurazione avanzata*

Suggerimento

Attualmente YaST supporta solo moduli per l'amministrazione di gruppi e utenti.

Suggerimento

Nel dialogo per la configurazione del modulo avete la possibilità di selezionare e modificare moduli di configurazione esistenti, crearne dei nuovi o creare e modificare dei template per questi moduli. Per modificare il valore all'interno di un modulo di configurazione o per cambiar nome ad un modulo, selezionate il tipo di modulo tramite il combo box al di sopra della rassegna del contenuto del modulo attuale. Nella rassegna vi è solo un elenco tabellare degli attributi consentiti in questo modulo e dei valori allocati. Qui trovate accanto agli attributi impostati anche altri attributi permessi per via dello schema utilizzato ma attualmente non abilitati. Se intendete copiare il modulo, modificate semplicemente `cn`. Per modificare i singoli valori degli attributi, selezionateli nella rassegna dei contenuti e cliccate su 'Modifica'. Si apre una finestra dialogo dove potete modificare le impostazioni dell'attributo. Con 'OK' rendete effettive le vostre modifiche.

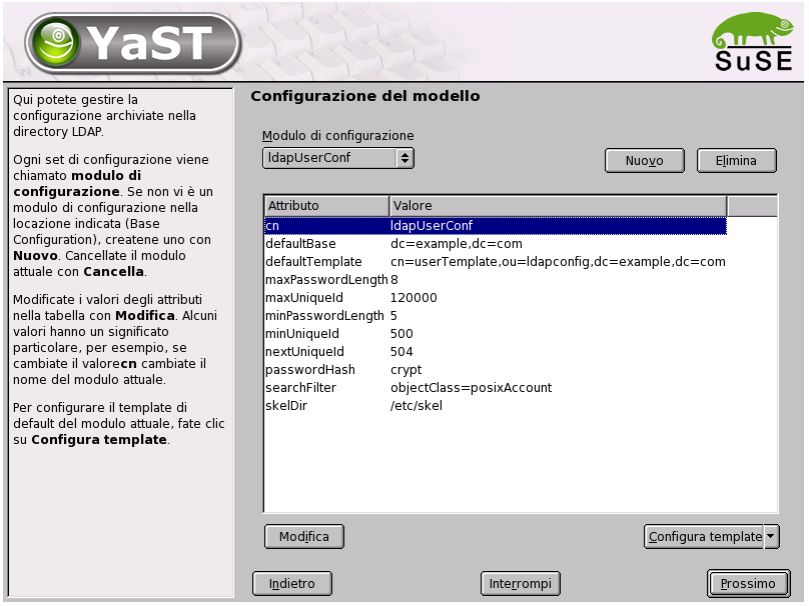


Figura 13.7: *YaST: configurazione del modulo*

Se volete aggiungere ai moduli uno nuovo, fate clic su 'Nuovo' al di sopra della rassegna dei contenuti. Nel dialogo che appare immettete la classe di oggetto del nuovo modulo (nel nostro caso `userConfiguration` o `groupConfiguration`) ed il nome del nuovo modulo. Se uscite dal dialogo con 'OK', il nuovo modulo viene inserito nella lista di selezione dei moduli esistenti e potrà essere selezionato e deselezionato tramite il combo box. Se volete cancellare il modulo attualmente selezionato, fate clic su 'Cancella'.

I moduli YaST per l'amministrazione di gruppi ed utenti integrano template con valori di default sensati se li avete definite in precedenza tramite il client LDAP di YaST. Per editare dei template fate clic su 'Configura template'. Verranno visualizzati nel menu a tendina template già esistenti che possono essere modificati o una registrazione vuota che vi porta comunque alla maschera per editare i template. Selezionatene uno ed impostate le caratteristiche del template nel seguente dialogo 'Configurazione template dell'oggetto'. Questo dialogo si compone di due finestre con sommari tabellari. Nella finestra superiore sono elencati gli attributi di template generali. Stabilitene i valori secondo il vostro scenario di impiego oppure lasciatene dei vuoti. Attributi "vuoti" vengono cancellati sul server LDAP.

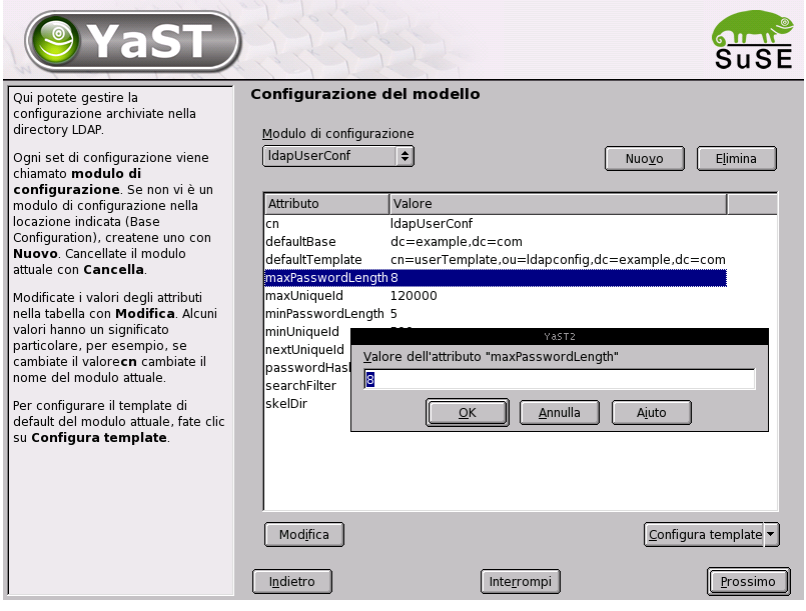


Figura 13.8: YaST: modificare gli attributi nella configurazione del modulo

Sotto ('Valori predefiniti per nuovi oggetti') vedete gli attributi del relativo oggetto LDAP (qui: configurazione dei gruppi e utenti), per i quali definite un valore di default. Potete aggiungere ulteriori attributi con valori di default, modificare coppie di attributi - valore e cancellare attributi interi. In egual maniera potete copiare un template modificando la registrazione `cn` per creare un nuovo template. Collegate il template con il relativo modulo impostando come descritto sopra il valore di attributo `defaultTemplate` del modulo sul DN del template adattato.

Suggerimento

Potete generare dei valori di default per un attributo da altri attributi utilizzando delle variabili al posto di valori assoluti. Esempio: `cn=%sn %givenName` verrà generato automaticamente dai valori di attributo di `sn` e `givenName`.

Suggerimento

Quando i moduli ed i template sono configurati correttamente e pronti ad essere utilizzati, create con YaST nuovo gruppi ed utenti.

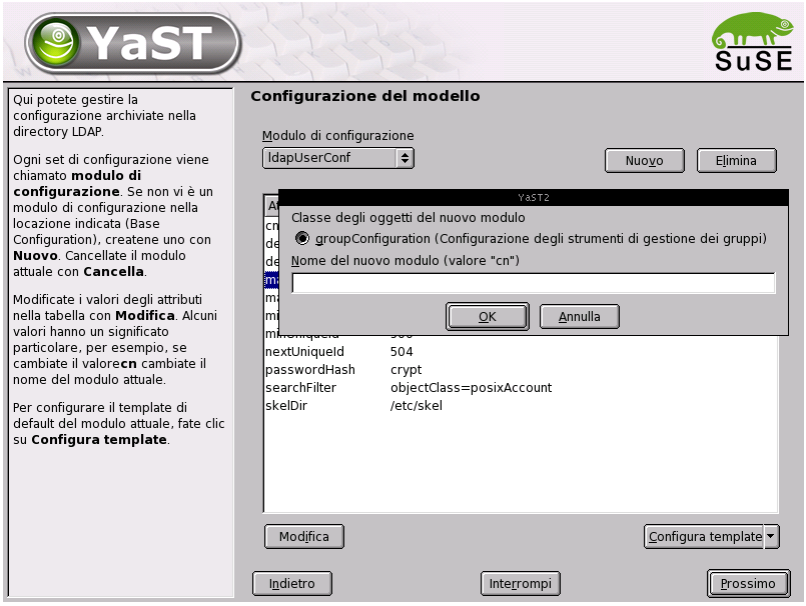


Figura 13.9: YaST: generare modulo nuovo

Utenti e gruppi– configurazione con YaST

Dopo aver configurato i moduli e template per la rete, vi accorgerete che il rilevamento dei dati degli utenti e dei gruppi si discosta solo minimalmente dalla procedura da seguire senza l'utilizzo di LDAP. Illustreremo di seguito brevemente l'amministrazione degli utenti, la procedura per l'amministrazione dei gruppi è simile.

Il modulo di amministrazione degli utenti di YaST si trova sotto 'Sicurezza & Utenti' → 'Modificare e creare utenti'. Se volete aggiungere un nuovo utente, fate clic su 'Aggiungi'. Si apre una maschera dove potete immettere i principali dati dell'utente come il nome, login e password. Dopo aver inserito i dati premendo il bottone 'Dettagli' potrete configurare in modo più mirato l'appartenenza al gruppo, shell di login e directory home. I valori di default per i campi di immissione sono stati stabiliti seconda la procedura descritta nella sezione *Moduli e template – configurazione con YaST* a pagina 371. Se avete abilitato l'uso di LDAP si apre una seconda maschera per l'immissione degli attributi di LDAP (vedi figura 13.12 a pagina 379). Selezionate gli attributi di cui intendete modificare i relativi valori e cliccate su 'Modifica' per aprire la finestra di immissione

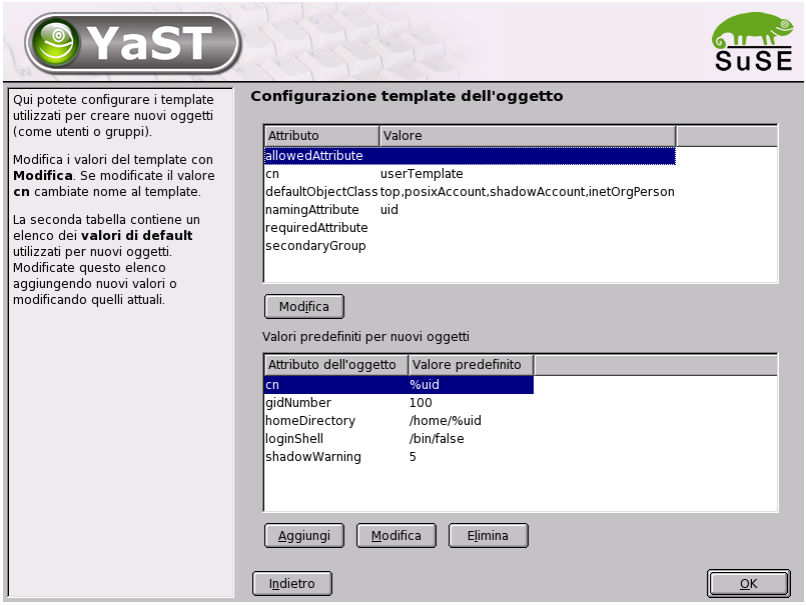


Figura 13.10: *YaST: configurare un template per l'oggetto*

relativa. Con 'Prossimo' uscite dalla maschera e ritornate alla maschera iniziale per l'amministrazione degli utenti.

Dalla maschera iniziale dell'amministrazione degli utenti (vedi figura 13.11 nella pagina seguente) il bottone 'Opzioni per esperti' vi dà la possibilità di applicare un filtro di ricerca LDAP agli utenti disponibili o di configurare il client LDAP di YaST per la prima volta tramite 'Configura il client LDAP'.

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.

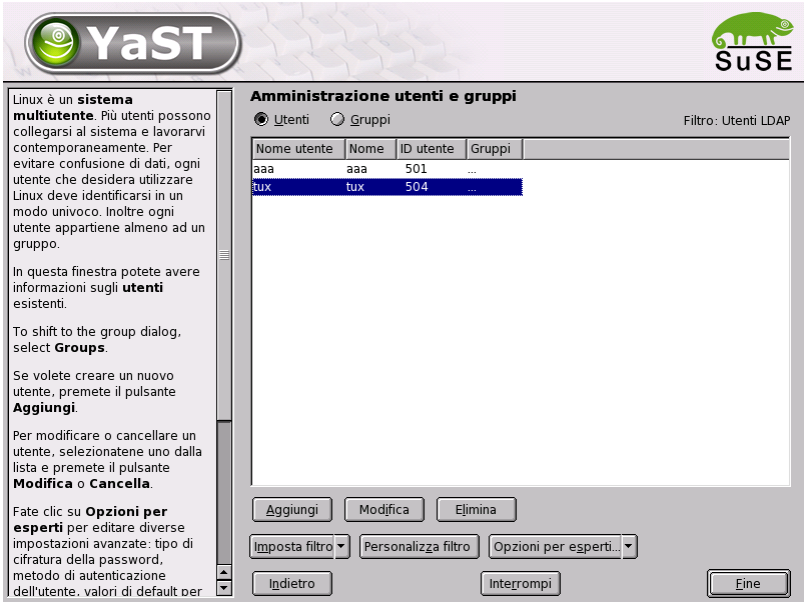


Figura 13.11: YaST: amministrazione utente

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 di tutti i principali settori della configurazione LDAP incl. 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 nei principi di base di LDAP. http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf

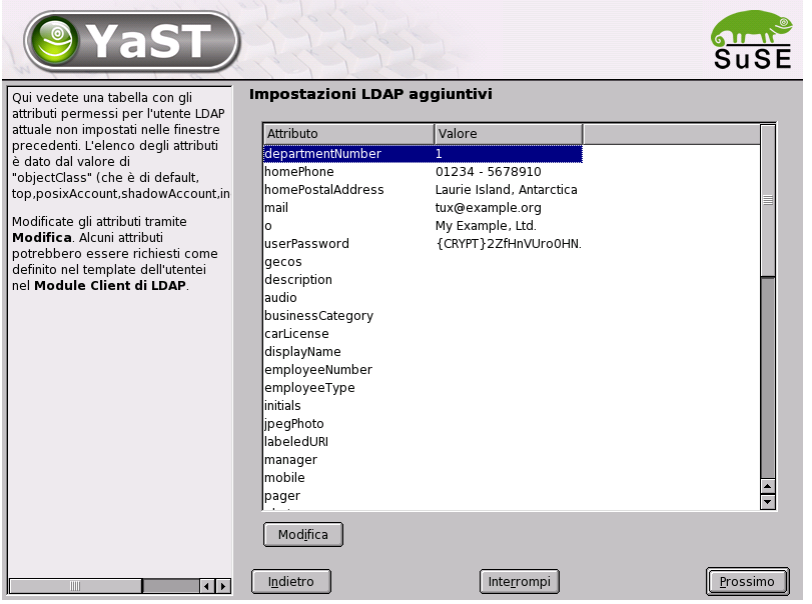


Figura 13.12: *YaST: impostazioni LDAP aggiuntivi*

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.

NIS – Network Information Service

Non appena diversi sistemi Unix intendono accedere a risorse comuni nella rete, si dovrà assicurare che non vi siano 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 trova 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 *NFS – file system dislocati* a pagina 385.

NIS (ingl. *Network Information Service*) può essere considerato un servizio database che permette l'accesso alle informazioni dei file `/etc/passwd`, `/etc/shadow` o `/etc/group` da ogni punto della rete. L'NIS può anche essere usato per compiti più complessi (ad esempio, per `/etc/hosts` o `/etc/services`), sui quali, tuttavia, non ci soffermeremo in questa sede. L'NIS è anche conosciuto come `'YP'`, dall'inglese *yellow pages*, ovvero *le pagine gialle* della rete.

Server NIS master e slave

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 (per 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. 13.13 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 richiedere poi i dati dal server NIS.

Se intendete integrare nella vostra rete ulteriori server NIS ("server slave"), dovrete attivare la box 'Esiste un server NIS slave attivo'. In aggiunta va attivata anche la casella 'Distribuzione veloce mappe' che trasmette rapidamente le registrazioni della banca di dati dal server master al server slave.

Se inoltre volete permettere agli utenti nella vostra rete di modificare le loro password (con il comando `yppasswd`, dunque non solo quelli locali, ma anche quelli che per il server NIS), potete impostarlo in questa maschera. Si attiveranno anche le checkbox 'Permetti di cambiare il campo GECOS' e 'Permetti di cambiare la shell'. "GECOS" significa che l'utente ha la possibilità di modificare le sue impostazioni del nome e indirizzo (con il comando `ypchfn`). "SHEL-

Figura 13.13: *YaST: tool di configurazione per server NIS*

L" vuol dire che può scegliere un'altra shell rispetto a quella di default (con il comando `ypchsh`, per esempio bash al posto di sh).

Cliccando su 'Altre impostazioni globali...' giungete ad un menu (Fig. 13.14 nella pagina successiva), in cui si può cambiare la directory sorgente del server NIS (di default `/etc`). Inoltre si possono unire password e gruppi. Le impostazioni vanno lasciate su 'Sì', in modo che non si creano delle incongruenze tra i file (`/etc/passwd` e `/etc/shadow` o `/etc/group` e `/etc/gshadow`). Inoltre si può stabilire l'ID minimo degli utente e gruppi. Facendo clic su 'OK', vi ritrovate nella maschera precedente. A questo punto fate clic su 'Prossimo'.

Se prima avete selezionato 'Esiste un server NIS slave attivo', dovete immettere i nomi dei computer che dovranno fungere da slave. Stabilite il nome è fate clic su 'Prossimo'. Se non avete 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 però volete 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. 13.15 a pagina 383). Di solito si trattaterà della vostra rete aziendale, in questo caso dovrebbero esserci le registrazioni

```
255.0.0.0 127.0.0.0
```

Figura 13.14: YaST: server NIS: modificare directory e sincronizzare file

```
0.0.0.0 0.0.0.0
```

La prima permette connessioni dal proprio computer, e la seconda permette a tutti i computer con accesso alla rete di inviare delle richieste al server.

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 *DHCP* a pagina 390. Se il client dispone di un indirizzo IP fisso, dovete immettere manualmente il dominio e server NIS (vd. Fig. 13.16 a pagina 384) . 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.

Figura 13.15: *YaST: server NIS: gli host con permesso di consultare il server*

Nelle impostazioni per esperti potete evitare che un host nella rete possa scoprire il server utilizzato dal vostro client. Se abilitate 'Broken Server' verranno accettate anche delle risposte da un server su una porta non privileggiata. Per maggiori dettagli consultate la pagina di manuale di `ypbind`.

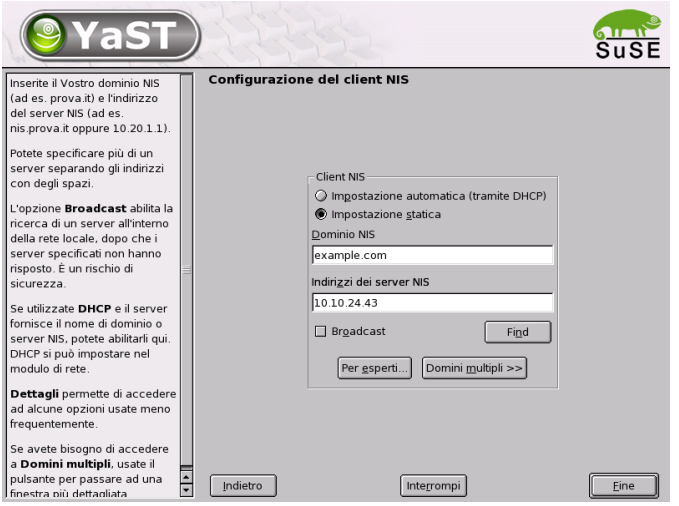


Figura 13.16: *YaST: client NIS: dominio e server NIS*

NFS – file system dislocati

Come abbiamo già accennato nel paragrafo 13 a pagina 380, l'NFS e l'NIS servono a rendere trasparente la rete per l'utente. L'NFS permette di dislocare i file system nella rete. Non importa su quale computer l'utente lavora, egli si troverà sempre di fronte allo stesso ambiente.

Sia l'NIS, che l'NFS sono servizi asimmetrici. Vi sono server NFS e client NFS, ma ogni computer può essere contemporaneamente sia l'uno che l'altro, ovvero può 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.

Importare file system con YaST

Ogni utente (se dispone dei relativi permessi), può montare directory NFS da un server NFS nel proprio albero di file. Il modo più semplice è di farlo con il 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. 13.17).

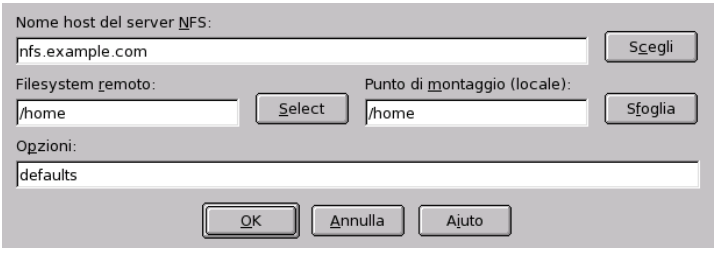


Figura 13.17: *Configurare il client NFS*

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 , che realizzate immettendo 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*⟩

Per importare, ad esempio, le directory degli utenti dal computer `sole`, usate il comando:

```
mount sole:/home /home
```

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. 13.18).

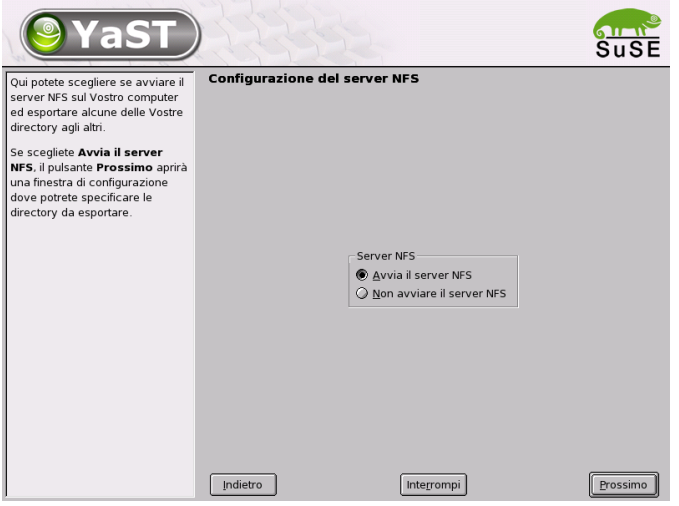


Figura 13.18: *YaST: tool di configurazione per server NFS*

Quindi, selezionate '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. 13.19 a fronte). 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 per il pacchetto `exports` (`man exports`).

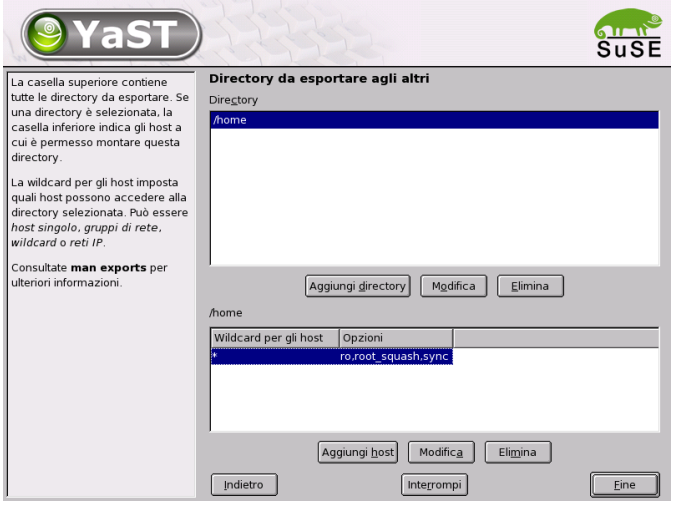


Figura 13.19: *YaST: server NFS: immettere directory da esportare e host*

Con 'Fine' concludete la configurazione.

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:

- Il portmapper RPC (portmap)
- Il demone di mount RPC (rpc.mountd)
- Il demone NFS RPC (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 possa accedervi e in che modo. Anche tutte le sottodirectory di un indirizzario esportato vengono esportate automaticamente. I computer che possono accedervi vengono solitamente indicati coi propri nomi (compreso il nome di dominio), ma è anche possibile usare dei simboli jolly `'*'` e `'?'`, che conosciamo dalla bash. Se non indicate alcun nome di host, saranno tutti i computer ad avere accesso a questa directory (con i diritti indicati).

I permessi con i quali una directory viene esportata sono riportati nella lista tra parentesi, dopo il nome del computer. I principali permessi di accesso sono descritti nella tabella successiva:

Opzioni	Significato
ro	Il file system viene esportato con il solo permesso di lettura (default).
rw	Il file system viene esportato con il permesso di lettura e scrittura.
root_squash	Questa opzione fa sì che l'utente `root` del computer in questione non disponga dei soliti diritti `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 del 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.

Tabella 13.14: *Permessi di accesso per directory esportate*

Il file `exports` potrebbe, ad esempio, essere simile al file 46.

```
#
# /etc/exports
#
/home            sole(rw)   venere(rw)
/usr/X11         sole(ro)   venere(ro)
/usr/lib/texmf   sole(ro)   venere(rw)
/                terra(ro,root_squash)
/home/ftp        (ro)
# End of exports
```

file 46: /etc/exports

Il file `/etc/exports` viene letto da mountd e nfsd. Se viene modificato, sia mountd che nfsd devono essere riavviati in modo da rendere effettiva la modifica apportata. Il modo più semplice per realizzare ciò è digitare il comando:

```
rcnfsserver restart
```

DHCP

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, invece di dover 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 nella rete possono essere integrati facilmente nella rete, ed assegnare 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.

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 usare, 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 dover configurare alcunché.

Per scenari più complessi, si può ricorrere al dhclient dell'ISC che potete amministrare tramite il file di configurazione `/etc/dhclient.conf`.

Il server DHCP dhcpd

Il *Dynamic Host Configuration Protocol Daemon* è il cuore di ogni sistema DHCP. Egli "affitta" 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`:

```
default-lease-time 600;         # 10 minutes
max-lease-time 7200;            # 2  hours

option domain-name "cosmo.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;
 }
```

file 47: *Il file di configurazione* `/etc/dhcpd.conf`

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 "affittato" 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). Sarebbe naturalmente ideale, se nel vostro sistema o sulla vostra rete, fosse già in esecuzione un server dei nomi che tenga in riserva anche un nome di host per indirizzi dinamici e viceversa. Ulteriori informazioni riguardanti la configurazione di un proprio server dei nomi vedi sezione 13 a pagina 344.
- `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 consegnati 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, contro ogni aspettativa, 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.

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, che quando non vi sono più sufficienti indirizzi liberi disponibili si rende necessaria una ridistribuzione degli indirizzi.

Per identificare un sistema con un indirizzo *statico*, il server DHCPD ricorre al cosiddetto indirizzo hardware: si tratta di un determinato numero 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 47 a pagina 391 viene aggiunta una registrazione come nel file 48, il DHCPD fornirà in ogni caso gli stessi dati al computer corrispondente.

```
host terra {
  hardware ethernet 00:00:45:12:EE:F4;
  fixed-address 192.168.1.21;
}
```

file 48: *Aggiunte al file di configurazione*

La struttura di queste righe è autoesplicativa:

Come prima cosa viene indicato il nome del computer da definire (host *nomehost*), 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.

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/`) su cui troverete ulteriori informazioni riguardanti DHCP come anche la documentazione per la 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 offerta 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 dei costi che da un punto di vista della sicurezza.

Sincronizzare l'orario con xntp

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 comunque 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.

Configurazione nella rete

In SuSE Linux, xntp è preconfigurato in modo che solo l'ora del sistema locale funge da 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 per 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 che presenta degli errori andrebbe ad influire sull'orario del vostro sistema.

xntpd può essere solitamente essere 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.

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 da più vicino. 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 per 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 pacchetto `xntp-doc` nella directory `/usr/share/doc/packages/xntp-doc/html`.

Il server web Apache

Che cosa è un server web?

Server web

Il server web fornisce le pagine `HTML` richieste da un client. Queste pagine possono trovarsi in una directory del server (cosiddette pagine passive o statiche) oppure venir generate in risposta ad una richiesta (contenuti attivi).

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). (Per degli approfondimenti, la l'attuale versione dell' HTTP 1.1 è documentata nell' RFC 2068 così come nell' Update RFC 2616. Gli RFC sono reperibili alla seguente URL: `http://www.w3.org` .)

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://` il *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 insieme compongono 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 (per esempio 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, per 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 per esempio nella sezione *DocumentRoot* a pagina 407.

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 constesto. Chiaramente potrete impostare se Apache debba servirsi di questo automatismo, e stabilire quali pagine includere in questo meccanismo. Nella sezione *DirectoryIndex* a pagina 408 viene illustrato come realizzare ciò.

Nel nostro esempio, immettendo

`http://www.suse.de`

il server fornirà la pagina

`http://www.suse.de/index.html`.

Che cos' è Apache?

Il server web più diffuso

Con una quota del 60 % (secondo `http://www.netcraft.com`) Apache è il server web più diffuso al mondo. Per applicazioni web, Apache viene spesso utilizzato in combinazione con Linux, la banca dati MySQL ed i linguaggi di programmazione PHP e Perl. Per questo tipo di combinazione si è forgiata l'abbreviazione "LAMP".

Alcuni dei vantaggi offerti da Apache:

Scalabilità

Tramite dei moduli potete arricchire Apache di 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.

Flessibilità

Potrete compilare dei moduli per adattare Apache anche alle vostre preferenze più insolite. Chiaramente questo pressupone un certo know-how ;-)

Stabilità

Apache è software open-source, e quindi il codice è stato testato da una miriade di programmatori che di volta in volta hanno eliminato degli eventuali errori di programmazione. Grazie a questa verifica, Apache (nell'ambito del possibile in tema di software) è esente da errori. Nonostante tutto non si può escludere che in futuro non vengano scoperte delle nuove falle nella sicurezza. Nella sezione *Sicurezza* a pagina 422 viene descritto dove poter reperire delle indicazioni utili riguardanti la sicurezza, e come porre rimedio in caso di necessità.

Le feature

Apache supporta una serie di utili feature di cui segue una breve rassegna.

Host virtuali (virtual hosts)

Il supporto di host virtuali consente che con una istanza di Apache e quindi su di un singolo server possono essere gestiti diversi siti web, laddove questo procedimento è trasparente all'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 il costo d'acquisto e l'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 (per esempio Lynx) viene fornita una versione semplificata delle pagine, senza frame. In questo modo si aggira il problema dovuto 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 di ciascun browser).

Gestione flessibile di errori

Se si verifica un errore (per esempio 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.

I principi

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 processare la 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) che si basa su Apache.

Le differenze tra Apache 1.3 e Apache 2

Sommario

Ecco le differenze principali tra Apache 1.3 ed Apache 2:

- Il modo di processare contemporaneamente diverse richieste. In Apache 2 si ha la scelta tra cosiddetti thread e processi. I processi vengono amministrati da un apposito modulo, il cosiddetto modulo multi-processing (MPM). La reazione di Apache alle richieste viene determinata 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 dover provvedere a questo aspetto. La sequenza nella quale vengono eseguiti i moduli, che prima dove 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 senza diritti 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

Vedi anche `http://httpd.apache.org/docs-2.0/en/`.

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", cioèla funzione con lo stesso input deve produrre sempre lo stesso risultato, indipendentemente dal numero di thread in esecuzione. Le funzioni devono essere quindi programmati 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.

Thread e processi

Mentre Apache 1.3 lancia un proprio processo per le richieste, Apache 2 esegue le richieste come processo proprio 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 *Installazione* a fronte) l'MPM da utilizzare.

Lo sviluppo del terzo modo, "perchild', non è ancora del tutto concluso, così in SuSE Linux non è (ancora) disponibile.

Il problema con Apache 2 è che non tutti i moduli sono stati ricompliati in modo da essere thread-safe. Se vi serve un modulo non ancora thread-safe non vi resta che continuare ad utilizzare Apache 1.3 oppure utilizzare l'MPM "prefork" sotto Apache 2.

Conclusione

Alla domanda quale versione di Apache si dovrebbe utilizzare, rispondiamo che se finora con Apache 1.3 tutto è andato bene e la disponibilità permanente delle pagine web per voi ha una certa priorità, consigliamo di aspettare ancora prima di eseguire il passaggio ad Apache 2. Questo vale anche se vi servono dei moduli che non sono stati ancora adattati ad Apache 2.

Se per voi la priorità consiste nel realizzare una più elevata performance oppure vi serve uno delle nuove feature di Apache 2 (per esempio il filtro) allora si dovrebbe effettuare il passaggio ad Apache 2.

Un ulteriore argomento a favore di Apache 2 è che vi è un apposito strumento di configurazione in YaST che vi permette di eseguire comodamente le vostre impostazioni.

In ogni caso si consiglia di eseguire dei test con una installazione di prova per vedere se il proprio sito web armonizza bene con Apache 2, prima di utilizzare Apache 2 effettivamente.

Installazione

Scelta di pacchetti in YaST

Per scenari meno complessi basta selezionare il pacchetto Apache. Si dovrà scegliere tra il pacchetto `apache` (Apache 1.3) o il pacchetto `apache2` (Apache 2). I rispettivi vantaggi e svantaggi delle due versioni sono illustrati nella sezione *Le differenze tra Apache 1.3 e Apache 2* a pagina 401. Coloro che non vogliono o non devono ricorrere alle nuove caratteristiche di Apache 2 vanno sul sicuro installando Apache 1.3 (il pacchetto `apache`).

Se installate pacchetto `apache2` dovete installare inoltre uno dei pacchetti MPM: il pacchetto `apache2-prefork` oppure il pacchetto `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 del pacchetto `mod_php4` sono "threadsafe".

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 `apache-example-pages` oppure il pacchetto `apache2-example-pages` è stato installato.

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 `mod_perl` per Perl, il pacchetto `mod_php4` per PHP ed infine il pacchetto `mod_python` per Python o i relativi moduli per Apache 2.

Come utilizzare questi moduli è illustrato nella sezione *Creare contenuti dinamici tramite moduli* a pagina 415.

Altri pacchetti utili

Inoltre è consigliabile installare la corposa documentazione che trovate nel pacchetto `apache-doc` o nel pacchetto `apache2-doc`. Per la documentazione vi è un alias (di cosa si tratta viene descritto nella sezione *Configurazione* nella pagina successiva), 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 `apache-devel` o il pacchetto `apache2-devel` come anche i relativi strumenti di sviluppo, tra cui gli strumenti `apxs` che vengono descritti più dettagliatamente nella prossima sezione *Installare moduli con Apxs* in questa pagina.

Installare moduli con Apxs

Uno strumento di sicuro interesse per sviluppatori di moduli è `apxs` o il suo equivalente in Apache 2, `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, `apxs` 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 `apxs` sono descritte nella relativa pagina di manuale.

Quali pacchetti servono per installare una delle versioni di `apxs` viene descritto nella sezione *Installazione* a pagina 403.

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 *Configurazione con SuSEconfig* in questa pagina.

Configurazione

É necessario configurare?

Dopo aver installato Apache dovete intervenire sulla configurazione solo se avete delle esigenze o preferenze particolari. Nella maggior parte dei casi Apache può essere utilizzato così come installato di default.

Apache si lascia configurare tramite SuSEconfig oppure editando direttamente il file `/etc/httpd/httpd.conf`, in questo caso dovete impostare la voce

```
ENABLE_SUSECONFIG_APACHE="yes"
```

che trovate sotto `/etc/sysconfig/apache2` su `no`, affinché SuSEconfig non sovrascriva le vostre modifiche fatte in `/etc/httpd/httpd.conf`.

Configurazione con SuSEconfig

Le impostazioni che potete effettuare sotto `/etc/sysconfig/apache` (e `/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 impostando la relativa variabile in `/etc/sysconfig/apache` su "yes" (Apache 1.3) o rispettivamente immettendo il nome del modulo nella lista della variabile `APACHE_MODULES` (Apache 2). 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 `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.

Configurazione manuale

Il file di configurazione

Il file di configurazione `/etc/httpd/httpd.conf` (risp. `/etc/apache2/httpd.conf`) vi consente di apportare delle modifiche che non è possibile realizzare tramite le impostazioni in `/etc/sysconfig/apache` o risp. 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 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. Questo valore (in Apache 1) viene modificato da SuSEconfig in base alla impostazione della variabile `HTTPD_PERFORMANCE`.

LoadModule

Le direttive `LoadModule` indicano i moduli da caricare. In Apache 1.3 i moduli vengono caricati nella sequenza indicata dalle direttive `LoadModule`. In Apache 2 la sequenza di caricamento viene stabilita invece dai moduli, vedi a riguardo la sezione *Le differenze tra Apache 1.3 e Apache 2* a pagina 401.

Inoltre, le direttive indicano i file contenuti dal modulo.

Port

Indica il port su cui Apache attende delle richieste. Di solito si tratta del port 80, il port standard per HTTP. In linea di massima non è consigliato modificare questa impostazione.

Un motivo per farlo potrebbe essere quello di voler provare una nuova versione aggiornata del sito web. In questo modo la versione del sito in funzione rimane raggiungibile tramite il port standard 80.

Un altro motivo potrebbe essere quello di voler rendere disponibili delle pagine solo su Intranet, perché contengono delle informazioni sensibili. In questo caso si imposta il port sul valore `8080` e si bloccano tutti gli accessi provenienti dall'esterno diretti a questo port 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 quando quando cercherà di 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 `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 *AccessFileName* a fronte.

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" (tutti gli accessi consentiti) a parte delle eccezioni
- "deny all" (tutti gli accessi negati) a parte delle eccezioni

Un esempio per il secondo approccio:

```
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 *AllowOverride* 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 *Host virtuali* a pagina 419) 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` (vedi a riguardo la sezione *Directory* a pagina 408).

ScriptAlias

Questa direttiva è simile ad `Alias`. Comporta inoltre che i file nella directory meta vengano trattati come script CGI.

Server Side Includes (SSI)

I cosiddetti server side include 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>
```

Apache in esecuzione

Dove deporre le pagine e script?

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 installati delle piccole pagine esempio che servono solo per vedere se Apache è stato installato correttamente e gira nel modo dovuto; questi file possono essere sovrascritti (meglio: cancellarli).

Propri script CGI si installato sotto `/srv/www/cgi-bin`.

Lo stato di funzionamento di Apache

Quando è in esecuzione Apache scrive i propri messaggi di log nel file `/var/log/httpd/access_log` o `/var/log/apache2/access_log`, dove viene documentata l'ora ed il metodo (`GET`, `POST`...) con il quale le risorse sono state richieste e messe a disposizione.

In caso di errore trovate le indicazioni attinenti nel file `/var/log/httpd/error_log` (nel caso di Apache2 sotto `/var/log/apache2`.

Contenuti dinamici

Sommario

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 di 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 dei tool della riga di comando in modo che accettano dell’input di Apache e glielo ritornano.
- 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 delle altre funzioni (per esempio 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.

Interprete di script sotto forma di modulo vs. CGI

Mentre gli script CGI vengono eseguiti quando invocati da Apache (in modo analogo alle chiamate dalla riga di comando), nel caso di moduli viene utilizzato un interprete embedded in Apache che gira continuamente. (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 la 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 di 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, ed così con il tempo si faranno sentire gli effetti di richieste negate o eventi simili ... .

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 tramite

```
<!--#echo var="DATE_LOCAL" -->
```

alla fine dell'inizio del commento `<!--` 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 nel eseguire una ricerca degli SSI nei file eseguibili. L'altra possibilità consiste di stabilire il tipo di file nei quali cercare gli SSI. Entrambi gli approcci vengono illustrati nella sezione *Server Side Includes (SSI)* a pagina 410.

CGI

Che cos'è 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 da ritornare in risposta una pagina personalizzata in base alla richiesta.

Vantaggi della CGI

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.

GET e POST

I parametri di immissione possono essere consegnati al 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.)

Linguaggi per CGI

In linea di principio i programmi CGI possono essere scritti in ogni linguaggio di programmazione. Di solito vengono utilizzati a tale scopo dei linguaggi di scripting (linguaggio interpretato) come Perl oppure PHP; per CGI dove l'accento è posto sulla velocità si propone C oppure C++.

Dove riporre gli script?

Apache si aspetta questi programmi in una determinata directory (`cgi-bin`). Questa directory si lascia impostare nel file di configurazione, vedi la sezione *Configurazione* a pagina 405.

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.

Creare contenuti dinamici tramite moduli

Moduli per linguaggi di scripting

Vi sono una serie di moduli per Apache.

Nota

Moduli

Il termine "modulo" ha due significati.

Da una parte vi sono moduli che possono essere integrati in Apache e assumere una determinata funzionalità, per 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 sono i moduli CGI presenti in tutti i linguaggi di programmazione che facilitano la programmazione di applicazioni CGI mettendo a disposizione dei metodi per leggere dei parametri di request e per emettere del codice HTML.

Nota

Tutti i seguenti moduli sono disponibili sotto forma di pacchetti in SuSE Linux.

mod_perl

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 *Installazione* a pagina 403). Le registrazioni necessarie per

Apache sono già incluse nel file di configurazione, vedi `/usr/include/apache/modules/perl/startup.perl` (Apache 1) o rispettivamente `/etc/apache2/mod\_perl-startup.pl` (Apache 2).

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` richiamandoli 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/"
```

mentre per `mod_perl` si ha:

```
<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:

- Con `Apache::Registry` tutti gli script vengono compilati e mantenuti nella cache. Ogni script viene generato come contenuto di una subroutine.

  Anche se ciò 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 vengono mantenute 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` si comporta in modo molto simile alla CGI. 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 in un determinato momento di uno script.)

Dunque con `Apache::PerlRun` non bisogna porre particolare attenzione ad una programmazione senza sbavature, dato che le variabili all'avvio dello script vengono reinizializzati e quindi non possono contenere dei valori risalenti a chiamate precedenti.

Per tale ragione `Apache::PerlRun` è più lento di `Apache::Registry`, ma comunque più veloce di CGI, visto che non bisogna lanciare un processo per l'interprete.

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/`

I pacchetti: il pacchetto `mod_php4-core` va installato in ogni caso. Per Apache 1 serve inoltre il pacchetto `mod_php4`, per Apache 2 il pacchetto `apache2-mod_php4`.

mod_python

Python è un linguaggio di programmazione orientato agli oggetti con un sintassi chiara e ben leggibile. Una particolarità di questo linguaggio è che la struttura del programma dipende dall'indentazione. I singoli blocchi non vengono demarcati da parentesi graffe (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/`

Installate il pacchetto `mod_python` o rispettivamente il pacchetto `apache2-mod_python`.

mod_ruby

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. Ruby fa pensare a Smaltalk in termini di concepimento.

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/`

Host virtuali

Hosting virtuale

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 dedicato. Apache è stato uno dei primi server web con supporto per 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 un sistema.

Illustreremo tutte e tre le possibilità.

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 le richieste in entrata. In seguito di devono configurare i singoli host virtuali:

```
<VirtualHost *>
    ServerName www.aziendauno.il
    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>
```

Nota: utilizzate `/var/log/apache2` al posto di `/var/log/httpd`, come percorso dei file di log per Apache 2.

Anche per il dominio ospitato in principio dal server (`www.aziendauno.it`) deve esservi una registrazione `VirtualHost`. Nel nostro esempio, lo stesso server gestisce accanto la domino originario un'ulteriore dominio (`www.aziendadue.it`).

Anche nelle direttive `VirtualHost`, come nel caso di `NameVirtualHost`, viene indicato un `*`. Apache mappa la richiesta agli host virtuale in base al campo host nell'intestazione HTTP. La richiesta viene fatta pervenire al 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.

Hosting virtuale basato sull'IP

Rassegna

In questo caso bisogna impostare diversi IP su di un sistema. Una istanza di Apache amministra diversi domini, laddove ogni dominio dispone di un indirizzo IP. Nel seguente esempio illustreremo come configurare Apache in modo che ospita oltre al suo indirizzo IP originairio `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 indirzzi 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.

Innanzitutto, si deve abilitare nel kernel l'aliasing di indirizzi IP, cosa che in SuSE Linux è già impostato di default.

Se il kerneI è stato configurato per consentire l'aliasing di indirizzi IP, tramite i comandi `ifconfig` e `route` si possono impostare ulteriori indirizzi IP. Per poter immettere questi comandi bisogna entrare nel sistema come `root`. Nel seguente esempio partiamo dal presupposto che il sistema ha già un proprio indirizzo IP, per esempio `192.168.1.10` assegnato al dispositivo di rete `eth0`.

L'IP utilizzato dal sistema si lascia visualizzare immettendo `ifconfig`. Ulteriori indirizzi IP si aggungono per 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 vi 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`.

Più istanze di Apache

Nei metodi fin qui descritti gli amministratori di un dominio possono leggere i dati di un altro dominio. 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 in base all' esempio di prima la direttiva sarà

```
Listen 192.168.1.10:80
```

Per le altre due istanze

```
Listen 192.168.1.20:80
```

e rispettivamente

```
Listen 192.168.1.21:80
```

Sicurezza

Ridurre il rischio di attacchi

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 essere in esecuzione alcun server.

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 ha 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 per esempio root.

Se si desidera dare agli utenti la possibilità di deporre dei file nella directory documento di Apache, invece di concedere l'accesso in scrittura a tutti, è preferibile creare una sottodirectory con accesso in scrittura, per 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. (per esempio `~/public_html`). In SuSE Linux questa funzionalità è abilitata di default, per ulteriori dettagli rimandiamo alla sezione *UserDir* a pagina 411.

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`

nel browser verranno visualizzati i file della directory `public_html` nella directory home dell'utente `tux`.

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 *Sicurezza* a pagina 425 sono elencati delle fonti per exploit e bugfix.

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 il file error-log, per vedere se dai messaggi si riesce ad individuare la causa del disturbo. L'error-log generale lo trovate sotto

  `/var/log/httpd/error_log` o risp. sotto `/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
  ```

  Nel caso di errori questo approccio si rileva essere molto utile anche all'avvio del server.

- Date una occhiata al bug database che trovate sotto

  `http://bugs.apache.org/`

- Abbonarsi a mailing list e newsgroup. La mailing list per utenti la trovate sotto

  `http://httpd.apache.org/userslist.html`

  come newsgroup consigliamo `comp.infosystems.www.servers.unix` e gruppi simili.

- Se le avete provate tutte senza risolvere il problema, e siete sicuri di trovarvi di fronte ad un baco di Apache, rivolgetevi a

  `http://www.suse.de/feedback/`

  in lingua inglese.

Ulteriore documentazione

Apache

Apache dispone di una documentazione esaustiva, come installarla sul vostro sistema viene descritto nella sezione *Installazione* a pagina 403. La troverete in seguito sotto

http://localhost/manual.

La documentazione aggiornata chiaramente la troverete sempre sulla home page di Apache:

http://httpd.apache.org

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/

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.

Il team di Apache sostiene una politica di informazione trasparente per quanto riguarda l'esistenza di bug 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 indicati se si tratta davvero di un problema non già rilevato), potete rivolgervi via e-mail a

security@suse.de

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/

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.

Software per la sincronizzazione dei dati

Nel caso di computer collegati costatemente 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.

Inter-Mezzo

L'idea che sta alla base di Inter-Mezzo 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.

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.

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.

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.

Criteri per scegliere il programma giusto

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 Inter-Mezzo.

L'alternativa è rappresentata da computer equiparati e che sincronizzano i loro dati a vicenda. Questo è l'approccio che segue unison.

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 della serie Unix e Windows.

Interattivo vs. automatico

Nel caso di InterMezzo la sincronizzazione dei dati avviene di solito automanticamente 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.

Velocità

unison e cvs vista l'interattività sembrano più lenti rispetto a intermezzo che lavora in background. cvs è in linea di massimo un pò più veloce di unison.

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 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'amminstratore di sistema che deve intervenire ed eventualmente eseguire a mano un rsync/scp) per ottenere la consistenza dei dati.

Selezione dei file e aggiunta di file

InterMezzo sincronizza l'intero file system. Nuovi file all'interno di un file system compaiono automanticamente 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.

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.

Volume dei dati e spazio richiesto sul disco rigido

Su ogni computer interessato serve abbastanza spazio per i dati distribuiti.

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.

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 installatoInterMezzo dovrebbe assolvere al suo compito in background.

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 dei 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.

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 ripara 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 un pò più complessa rende la configurazione . Senza SSL si dovrebbe utilizzare impiegare InterMezzo solo in reti protette e affidabili.

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.

Introduzione ad Inter-Mezzo

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

	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	+	++	+

Tabella 15.1: *Feature dei tool di sincronizzazione – = molto scarso, - = scarso o non presente, o = mediocre, + = buono, ++ = molto buona, x = presente*

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,per esempio 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 per esempio in una rete collegata via cavo protetta da un firewall.

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
```

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.cosmo.com
```

Al posto di `sole.cosmo.com`va naturalmente immesso il nome di rete del server. Si consiglia inoltre di creare dei file system della stessa dimensione su ogni computer.

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/
```

Introduzione ad unison

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.

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.

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:	Server:
`/home/tux/dir1`	`/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 sono state 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, per esempio `~/.unison/example.prefs`:

```
root=/home/foobar/dir1
root=ssh://fbar@server//homes/fbar/dir2
batch=true
```

file 49: *Il file* `~/.unison/example.prefs`

Per inizializzare la sincronizzazione basta semplicemente indicare il file come argomento della riga di comando:

```
unison example.prefs
```

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.

Introduzione a CVS

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 per esempio unison sarebbe pensabile anche questo scenario:

A > B > C > S

A, B, C sono computer che possono elaborare i dati in questione.

Impostare un server CVS

Sul "server" si trovano tutti i dati validi, ovvero soprattutto la versione attuale di ogni file. Anche per esempio una postazione di lavoro fissa può fungere da server. E' consigliabile di 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, per esempio

```
cvs import -m 'questa è una prova' synchome tux tux_0
```

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 modificate 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.

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/
```

Introduzione a mailsync

Campo di impiego

Mailsync assolve principalmente tre compiti:

- sincronizza e-mail localemente memorizzati con e-mail memorizzate 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

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 per esempio 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 nome 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 i lati
- 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 i lati 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 esisteva sull' altro lato 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.

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, cioènon 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`.

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.

16

Reti eterogenee

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.

Samba

Con Samba è possibile trasformare un qualsiasi computer Unix in un server di file e stampa performante per computer 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 — e dall'altra da documentazione ed esempi che trovate sotto `/usr/share/doc/packages/samba`, dopo aver installato Samba. Nella sottodirectory `examples` trovate anche la configurazione esempio commentata `smb.conf.SuSE`.

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 collegarsi ad una rete Microsoft. Samba implementa il protocollo SMB su TCP/IP. Così su ogni client deve essere installato il protocollo TCP/IP. Noi consigliamo di utilizzare esclusivamente TCP/IP sui client.

NetBIOS

NetBIOS è un'interfaccia software (API) progettata per la comunicazione tra computer; viene messo a disposizione un (ingl. *name service*) ai fini della identificazione reciproca degli host. Non vi è una istanza centrale ad assegnare i nomi, ogni computer 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) della 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 -"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 computer 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 di 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.

Installazione e configurazione del server

Se volete utilizzare pacchetto `samba` come server, installate il pacchetto 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`. Da un punto di vista logico il file di configurazione `/etc/samba/smb.conf` 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.

I parametri selezionati vengono spiegati in seguito.

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 da altri sistemi in una rete Windows.

workgroup = TUX-NET Con questa istruzione assegnate il server Samba ad un gruppo di lavoro. Adattate TUX-NET ai gruppi di lavoro esistenti 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, se il nome non è 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 `man smb.conf`.

os level = 2 In base a questo parametro il server Samba decide se tentare di fungere da LMB (ingl. *Local Master Browser*) per il proprio gruppo di lavoro. Il valore utilizzato nell'esempio è stato scelto volutamente basso, per evitare che in una rete Windows si verifichino dei disturbi dovuti ad un server Samba configurato in modo errato. I dettagli su questo tema importante si trovano nei file BROWSING.txt e BROWSING-Config.txt nella sottodirectory `textdocs` della documentazione del pacchetto.

Se ancora non gira un server SMB — per esempio 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 (per esempio 65), per fargli assumere il ruolo dell'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 cancellando il punto e virgola e adattare l'indirizzo IP.

I vostri sistemi Windows sono in esecuzione in sottoreti separate devono essere visibili tra di loro, nella vostra rete Windows *non* vi è un server WINS ed il vostro server Samba deve assumere il ruolo di server WINS: per fare questo attivate la riga con wins support = yes. Assicuratevi assolutamente che questo parametro sia attivato solo sul server Samba. In questa constellazione `wins server` non può essere utilizzato.

Le share

Nei seguenti esempi vengono condivisi il lettore di CD-ROM e le directory degli utenti, gli `homes`.

```
[cdrom]

    ;[cdrom]
    ;       comment = Linux CD-ROM
    ;       path = /media/cdrom
    ;       locking = no
```

file 50: *Sharare il lettore di CD-ROM*

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 i ';' a inizio riga.

- [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` si esporta 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 [home] vale: se un utente sul server di file Linux ha un valido account ed una propria directory home, il suo client si può collegarsi immettendo un login e una password validi.

```
[homes]
        comment = Home Directories
        valid users = %S
        browseable = no
         read only = No
        create mask = 0640
        directory mask = 0750
```

file 51: *Sharare gli home*

- `[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 dal nome della share, una volta stabilito il collegamento. Visto che nel caso della share `[homes]` è identico al nome dell'utente, gli utentcchemessi sono ristretti al proprietario della directory utente. Questa è un modo per consentire l'accesso solo ai proprietari.
- `browseable = no` con questa impostazione la share [homes] non è visibile nell'elenco delle share.

- `read only = No` Di default, Samba proibisce 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 computer 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:** Qui viene attribuita una password ad una share. Chi la conosce, ha accesso alla share.
- **User Level Security:** Questa variante introduce il concetto di utente. Ogni utente deve fare il login sul server con una password. Dopo di ciò il server può, secondo il nome dell'utente, accordare l'accesso alle singoli share esportate.
- **Server Level Security:** Samba dice 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 leggete il file `textdocs/security_level.txt`. Se amministrate diversi server su di un sistema impostate i parametri `interfaces` e `bind interfaces only`.

Suggerimento

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. Nell'URL di un browser, inserite `http://localhost:901` e fate il login come root. Badate che swat è abilitato anche nei file `/etc/xinetd.d/samba` e `/etc/services`, modificate la seguente riga: `disable = no`. Per maggiori informazioni su swat consultate la pagina di manuale di `swat` (`man swat`).

Suggerimento

Samba come server per il login

In reti composte principalmente da client Windows è spesso auspicabile che gli utenti possano fare 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 52:

```
[global]
 workgroup = TUX-NET
 domain logons = yes
 domain master = yes
```

file 52: *Sezione globale in smb.conf*

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 prodotti seguenti - il server Samba deve essere in grado di amministrarle, cosa che avviene tramite la registrazione encrypt passwords = yes nella sezione [globals]: 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:

```
useradd -m nome-dell'-host\$
smbpasswd -a -m nome-dell'-host
```

file 53: *Creare un account macchina*

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.

```
add user script = /usr/sbin/useradd -g machines \
  -c "NT Machine Account" -d \
  /dev/null -s /bin/false %m\$
```

file 54: *Creare automaticamente un account macchina*

Nella autenticazione qui impostata, i dati dell'utente vengono archiviati in `/etc/samba/smbpasswd`. Se volete archiviare i dati degli utenti su un server LDAP, tramite YaST | System | Editor per /etc/sysconfig | Servizi di rete | Samba dovete impostare la variabile `SAMBA_SAM` su `ldap` ed invocare SuSEconfig – moduli samba.

Installazione dei client

I client possono raggiungere 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 for Workgroups tale supporto non viene però installato con l'installazione standard. Per installare successivamente TCP/IP, si seleziona 'Aggiungere...' nell'applet di rete sotto Risorse di sistema alla voce '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.

Suggerimento

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.

Suggerimento

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` (`man smb.conf`) nella sezione socket options e nella pagina di manuale di `socket(7)` (`man socket(7)`). Ulteriori approcci vengono descritti in `textdocs/Speed.txt` e `textdocs/Speed2.txt`.

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.

Suggerimento

Il Samba-Team fornisce con `textdocs/DIAGNOSIS.txt` istruzioni da seguire passo dopo passo per controllare la configurazione.

Suggerimento

Netatalk

Con il pacchetto `netatalk`, potrete realizzare un potente server per file e stampante su client OS per Mac: è possibile accedere da un Macintosh ai dati di un computer Linux o stamparli tramite una stampante collegata.

Netatalk è un pacchetto 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). In principio, 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 `nslookup` (DNS, Domain Name Service), viene usato il comando `nbplkup` (NBP, Name Binding Protocol) e 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 ai programmi ifconfig e routed;
- 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 mette a disposizione la stampante nella rete (AppleTalk).

Potete esportare senza problemi 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. 13 a pagina 385). Back-up ed amministrazione dei permessi degli utenti possono essere amministrati centralmente dal server Linux.

Considerate che:

- a causa della restrizione dei client Macintosh, le password degli utenti sul server possono avere 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.

Dovete installare il pacchetto `netatalk` .

Configurazione del server di file

Nella configurazione standard, per gli utenti registrati sul sistema Linux, "Netatalk" è già funzionante al 100% come server di file. Per poter usufruire delle sue proprietà, dovrete eseguire alcune impostazioni nei file di configurazione che troverete nell'indirizzario `/etc/atalk`.

Tutti i file di configurazione sono puri file di testo. Le righe con un rombo `'#'` iniziale e le righe vuote vengono ignorate ("commenti").

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`, e qui è sufficiente l'impostazione di un unico valore.

```
eth0
```

(come nel file-esempio). Configurate qui altre interfacce, p.e. nel caso che usiate contemporaneamente più schede di rete. Se viene inizializzato il server, questi cerca nella rete le zone e 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 afpd.

Definire il server di file – afpd.conf

Il file `afpd.conf` definisce come debba apparire il vostro server di sui computer Mac-OS nel menù di 'Scelta'. Come gli altri file di configurazione, anche questo contiene commenti dettagliati che spiegano le varie opzioni.

Se qui non eseguite alcuna modifica, viene avviato solo il server di default e mostrato nella 'Scelta' con i nomi degli host. In questo caso non vi è quindi alcuna necessità di impostare valori, mentre è possibile 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. Se volete che anche altri server AppleShare (sullo stesso computer) usino TCP, dovete attribuire loro determinate porte. Accedere ai servizi tramite TCP/IP permette anche l'accesso al server anche tramite reti non-AppleTalk come, p.e., 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 12 000. In questo modo è raggiungibile anche con router TCP/IPD.

Nel file `AppleVolumes.default` (che spiegheremo dettagliatamente più avanti) viene stabilito quali directory (residenti sul server) del rispettivo server AppleShare vengano messe a disposizione come "volumi" di rete (= directory raggiungibili tramite la 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

Qui definite quali siano le directory da esportare. I permessi di accesso vengono stabiliti per mezzo dei consueti permessi degli utenti e dei gruppi di Unix.

Tale configurazione avviene nel file `AppleVolumes.default`.

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, invece di `access=`, si dice `allow:` (un sintomo caratteristico, sarebbe la visualizzazione – sul client Mac su AppleTalk – delle opzioni invece della denominazione stessa 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 portare dal back-up le vecchie impostazioni nei nuovi file e di rinominare quindi i nuovi file. In questo modo, approfittate anche degli attualissimi e dettagliati commenti dei file di configurazione.

Nota

Assieme a `AppleVolumes.default`, possono venire creati altri file come p.e. `AppleVolumes.guest`, utili a determinati tipi di 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 determinati utenti 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 ha la possibilità di fare il login sul server stesso.

Per la raffigurazione delle resource-fork di file tipiche per Mac OS, Netatalk crea delle directory `.AppleDouble` nel file system di Linux. Con l'opzione `noadouble` potete stabilire che queste directory vengano create solo se sono veramente necessarie. Sintassi:

```
/usr/local/guests "Guests" options:noadouble
```

Le spiegazioni contenute nel file stesso vi aiuteranno a trovare altre opzioni e possibilità.

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 dover indicare esplicitamente ogni singolo utente. 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 impostazioni in questo file completano quelle dei file del server `AppleVolumes.system` e `AppleVolumes.default`, per rendere possibile ulteriori attribuzioni individuali type/creator e per accedere ai file system. Queste impostazioni sono completamenti che impediscono all'utente registrato accessi non autorizzati dal server.

Il file `netatalk.pamd` serve all'autenticazione tramite PAM (Pluggable AuthenticationModules), ma al momento non ci interessa.

Attribuzioni di file – `AppleVolumes.system`

Nel file `AppleVolumes.System` stabilite quali attribuzioni type e 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 una impostazione. Se doveste aver problemi ad aprire, sotto Mac OS, un file di testo di un altro sistema (o viceversa), controllate le impostazioni lì contenute.

Configurazione del server di stampa

Nel file `papd.conf` viene messo a disposizione un servizio laserwriter. La stampante deve già funzionare localmente con l'lpd. 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 impostare niente in `papd.conf`, poichè, senza ulteriori indicazioni, gli incarichi di stampa vengono semplicemente inoltrati al demone della stampante `lpd`. La stampante si fa riconoscere nella rete AppleTalk come laserwriter. Potete però impostare anche una determinata stampante nel file di configurazione:

```
Ricezione_stampante:pr=lp:pd=/etc/atalk/kyocera.ppd
```

Questi parametri fanno apparire, nella selezione, la stampante con il nome Ricezione_stampante. Il corrispondente file di descrizione della stampante si trova generalmente dal produttore. Oppure, prendete il file `Laserwriter` dalla cartella 'Estensioni del sistema'; in questo modo, però, spesso non potete usufruire di tutte le proprietà della stampante.

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 ovvero 'sottofondo?; occorre circa un minuto, prima che le interfacce AppleTalk siano configurate ed accessibili. Con una richiesta di stato potrete vedere se il processo è terminato (lo riconoscerete da `OK` emesso tre volte):

```
terra:~ #  rcatalk status
```

"Checking for service atalk:OKOKOK"

Passate ora ad un Mac che giri su Mac OS. Controllate che Apple Talk sia attivato, selezionate 'Filesharing', eseguite un doppio clic su 'Apple share'; 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' e registrando l'indirizzo IP corrispondente, eventualmente seguito da due punti e il numero di porta.

Ulteriori informazioni

Per sfruttare appieno tutte le possibilità offerte dal pacchetto `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 viene usato 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/
- http://cgi.zettabyte.net/fom-serve/netatalk/cache/1.html

E come stanno le cose, viste in senso inverso? Si può accedere ad un drive AppleShare su Linux? La nostra risposta è: meglio di no, dal momento che il pacchetto corrispondente si trova ancora in uno stadio pre-alfa. I più coraggiosi lo trovano all'indirizzo: http://www.panix.com/~dfoster/afpfs/

Emulazione Netware con MARSNWE

L'emulatore Netware MARSNWE può sostituire in modo relativamente facile un server Novell-Netware 2.2 o 3.11 per servizi di file e stampa ed essere usato, allo stesso tempo, come router IPX. Tuttavia, per avere la piena funzionalità delle più recenti versioni di Netware, come, ad esempio, NDS (ingl. *Netware Directory Services*), dovrete ancora ricorrere all'originale. Con l'emulatore Netware MARSNWE ed un paio di modifiche minime, una postazione di lavoro che gira su DOS o Windows, già configurata per un server Netware 2.2/3.11/3.12, può usare anche un server Linux. L'amministrazione è meglio sbrigarla da Linux, dal momento che i programmi Novell non sono del tutto adatti all'amministrazione di sistema e inoltre bisogna anche fare attenzione alle licenze.

Lanciare l'emulatore Netware MARSNWE

MARSNWE di SuSE Linux può essere lanciato subito dopo l'installazione, dal momento che è stato preconfigurato in modo da poter essere subito usato. 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. Per il numero di rete e protocollo andate sul file di configurazione ampiamente commentato `/etc/nwserv.conf`. Inizializzate MARSNWE con il comando `rcnwe start`. Se appare la scritta `done` in verde al margine destro dello schermo, vuol dire che il programma è stato avviato con successo.

Con `rcnwe status`, verificate se l'emulatore è in esecuzione. Con `rcnwe stop`, lo fermate.

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 1-22, anche se non le useremo tutte. 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 path degli indirizzari sul server. Ci possono essere ancora tutta una serie di opzioni, indicate 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 configurato. 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
```

Inserire il numero di rete Netware e il protocollo attraverso il quale debba essere collegato a quale interfaccia di rete. Se si hanno più schede di rete e le si registra con numeri di rete diversi, vi verrà creata una route con IPX.

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 fissato sull'utente root.

Login dell'utente (Section 13):

```
13   LINUX           linux
```

Attribuzione degli utenti Netware agli utenti Linux. Potete anche usare questa section per immettervi una password.

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".

Queue della stampante (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 del pacchetto `ncpfs` .

Accesso ai server Netware e la loro amministrazione

Il pacchetto `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 nelle 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 da un server Netware in Linux, e `ncpumount`, per fare l'umount 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.

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 gli strumenti del pacchetto `ncpfs`.

Internet

Su Internet ci sono tante cose da dire. In questo manuale ci limiteremo a trattare due temi: la configurazione manuale di un accesso ADSL, per il caso dovessero verificarsi delle difficoltà durante la configurazione con YaST e la configurazione del proxy Squid.

smpppd come assistente di selezione

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 vuole controllare meglio il collegamento o tramite un applet ovvero un miniprogramma di KDE o anche 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 si vorrebbe monitorare il collegamento ad un computer raggiungibile via rete.

Ed è qui che entra in gioco smpppd 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 workstation con una propria sottorete privata.

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 il controllo 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 controllare 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 che all'interno di questa area hanno il permesso di accedere a smpppd e invece 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 la pagina di manuale di `smpppd` (`man 8 smpppd`) e la pagina di manuale di `smpppd.conf` (`man 5 smpppd.conf`).

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 la pagina di manuale di `smpppd-c.conf` (`man 5 smpppd-c.conf`) e la pagina di manuale di `cinternet` (`man 8 cinternet`).

Configurazione di un collegamento ADSL / T-DSL

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 `ppp` e `smpppd` 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 persmpppd (SuSE meta-ppp-deamon) ed i suoi front-end kinternet e cinternet. Vd. la pagina di manuale di `smpppd` (`man 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 staccare la connessione.

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, dopo 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. Questo però conviene solo se avete una flat

rate, ovvero canone fisso. Se pagate in base alla durata della connessione, fate attenzione che non vi sia un processo periodico (ingl. *cron job*) che vi colleghi ad Internet in continuazione, appesantendo in tal modo sensibilmente la vostra bolletta telefonica. Benché le flat rate prevedano anche collegamenti permanenti, conviene spesso collegarsi solo per determinati periodi e quando necessario:

- 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 può diventare rischioso, dal momento che qualcuno potrebbe tentare dalla rete ad individuare sistematicamente dei punti deboli del vostro sistema. Una connessione puntuale e che si serva di 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/dsl-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` (inglese)

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 su carico della cache con l'aiuto di programmi come Calamaris e cachemgr o come filtrare contenuti web con squidGuard.

Cos'è una cache-proxy?

Squid funge da cache-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.

Suggerimento

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.)

Suggerimento

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.

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 una cache proxy. 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 17 a pagina 482.

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 proxy dell'ISP.

L'intera comunicazione viene controllata da ICP (ingl. *Internet Cache Protocol*), che è basato sul protocollo UDP. Lo scambio di dati fra le cache avviene tramite HTTP (ingl. *Hyper Text Transmission Protocol*) che si basa su TCP.

Per trovare il server più appropriato per gli oggetti desiderati, la cache invia una richiesta ICP a tutti i proxy della stessa gerarchia. Se l'oggetto è stato trovato, i proxy rispondono tramite risposte ICP alle richieste con il codice "HIT"; se non è stato trovato nulla, rispondono con il codice "MISS". Nel caso di più risposte HIT, il server proxy incaricherà un server ad eseguire il download: questa decisione viene determinata fra l'altro dalla cache che invia come prima la risposta o dalla prossimità della cache. Se non viene inviata alcuna risposta soddisfacente, la richiesta viene inviata alla cache superiore.

Suggerimento

Per evitare la memorizzazione molteplice di oggetti in diverse cache della nostra rete, vengono usati altri protocolli ICP come p.e. CARP (ingl. *Cache Array Routing Protocol*) o HTCP (ingl. *Hyper-Text Cache Protocol*).

Più oggetti si trovano nella nostra rete, più grande è la possibilità di trovare quello cercato.

Suggerimento

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 per esempio indicano oggetti da non memorizzare temporaneamente.

Gli oggetti nella cache di solito vengono sostituiti a causa della mancanza di spazio di memoria attraverso algoritmi del tipo LRU (ingl. *Last Recently Used*) che sono stati concepiti per sostituire oggetti della cache. Il principio è quello di sostituire come primo gli oggetti meno richiesti.

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.

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 `1 MB/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 il di solito 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 (ingl. *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 *cachemgr.cgi* a pagina 486 .

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 giraSquid.

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. paragrafo 17 a pagina 480.

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 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.

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.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 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 diventa uno 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 poter essere usate, le ACL devono essere state 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 indicazioni: il nome `<acl_name>` può venire scelto liberamente. Per `<type>` è possibile scegliere fra una quantità 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.

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 *Il kernel Linux* a pagina 257.

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`.

Ora dovete solo salvare la nuova configurazione, compilare ed installare il nuovo kernel; eventualmente va anche riconfigurato LILO, ed infine riavviate il sistema.

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:

```
#
# 15.)
# Quale accesso ai singoli servizi deve venire deviato 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 deviare in
# maniera trasparente, il traffico web entrante ad un server web
```

```
# sicuro.
#
# Scelta: non eseguire alcuna registrazione o usare la sintassi
# delle regole di deviazione spiegata qui di seguito e divisa da
# uno spazio vuoto. Una regola di deviazione 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"
#
```

file 55: *Opzione 15 della configurazione del firewall*

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 "deviate" o 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 (Port 21), HTTPS o SSL (Port 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 *Avviare Squid* a pagina 475. 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`:

```
nmap -O indirizzo_IP
```

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: se questo non è il caso dobbiamo immettere: `rcapache start`

Così Apache viene lanciato con le impostazioni di default di SuSE Linux. In questo manuale Apache viene trattato in modo dettagliato.

Infine, dobbiamo copiare il file `cachemgr.cgi` nella directory `cgi-bin` di Apache:

```
cp /usr/share/doc/packages/squid/scripts/cachemgr.cgi
/usr/local/httpd/cgi-bin
```

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 contenute le seguenti regole:

```
http_access allow manager localhost
http_access deny manager
```

La prima ACL è la più importante, poiché il cache manager cerca di comunicare con Squid tramite il protocollo cach_object.

Le seguenti regole partono dal presupposto che il server web e Squid girino sullo stesso computer. La comunicazione fra il cache manager e Squid origina nel server web e non nel browser. Se quindi il server web si trova su un altro computer, dobbiamo aggiungere appositamente una ACL come nel seguente file esempio 56.

```
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
```

file 56: *Regole di accesso*

Inoltre servono le seguenti regole del file 57.

```
http_access allow manager localhost
http_access allow manager webserver
http_access deny manager
```

file 57: *Regole di accesso*

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 "Access-Controller-PlugIn" 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 la deviazione, 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" e che si basa 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 pacchetto `squidgrd`. 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 a Squid di impiegare SquidGuard. A questo scopo, usiamo nel file `/etc/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 deviazione, 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
```

Ore 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 esempio comune:

```
cat access.log.2 access.log.1 access.log | calamaris -a -w \
 >/usr/local/httpd/htdocs/Squid/squidreport.html
```

Il rapporto viene archiviato nella directory del server web. E di nuovo è necessario Apache per poter visualizzare i rapporti!

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/`

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 pacchetto `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 in cui lo scambio di dati viene 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.

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 (spesso chiamati gateway) i pacchetti che non sono destinati ad una delle proprie interfacce di rete. Con i filtri dei pacchetti presenti nel kernel di Linux è possibile controllare esattamente quali pacchetti della trasmissione di dati possano 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 sè stantepacchetto `SuSEfirewall2` inteso a facilitare l'impostazione di questi criteri.

La configurazione di SuSEfirewall2 è molto flessibile ed perciò adatta anche alla creazione di strutture più complesse di filtra pacchetti.

Il pacchetto filtra pacchetti permette di usare un computer Linux - tramite masquerading - come router per collegare 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

I principi del masquerading

Masquerading è la versione Linux di NAT; NAT significa 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 agli 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 dovrebbero essere configurati in modo da inviare i pacchetti destinati all'esterno a questo gateway.

Nota

Quando configurate la vostra rete, fate attenzione alla concordanza degli indirizzi broadcast e maschere 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! Modificate la variabile `IP_FORWARD` che si trova nel file `/etc/sysconfig/network/options` in `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 nella vostra rete interna, nascosto dietro il vostro router. Da qui il termine "masquerading"(mascheramento).

Il router, quale destinazione di una pacchetto risposta, deve identificare i pacchetti in entrata, modificare l'indirizzo di destinazione e inoltrarlo all'host nella rete locale.

Questo riconoscimento di pacchetti appartenenti a collegamenti creati dal router tramite masquerading avviene con l'aiuto di una tabella depositata 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 i comandi `ipchains` e `iptables`. Per avere indicazioni più precise, consultate le rispettive pagine di manuale di questi comandi. Per l'identificazione di singoli collegamenti masquerade, 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 "celare" contemporaneamente migliaia di collegamenti per ognuno dei vostri computer locali.

Poichè il percorso dei pacchetti entranti dipende dalla tabella di masquerading, non ci sono possibilità di aprire un collegamento dall'esterno all'interno: questo collegamento non è previsto nella tabella. Nella tabella, ogni collegamento effettuato ha un stato ben determinato, 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.

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 di pacchetti regola un 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 entrare nella vostra rete. È per esempio consigliabile intercettare quei pacchetti che utilizzano il servizio telnet sulla 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 finché 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.

Una struttura più efficace, anche se più complessa, potrebbe essere anche caratterizzata da una combinazione di diversi sistemi, come, p.e., la combinazione di un filtra pacchetti ed 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 tale proxy, è Squid, un server proxy http, la cui raggiungibilità va configurata nel vostro browser, affinché le richieste di pagine HTML vengano replicate dalla memoria del proxy, anzicché dall'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 pacchetto `howtoen`. Se questo pacchetto è stato installato, può venire letto con il comando `less /usr/share/doc/howto/en/Firewall-HOWTO.gz`.

SuSEfirewall2

Configurare il SuSEfirewall2 è più complesso e richede più esperienza. Sotto `/usr/share/doc/packages/SuSEfirewall2` trovate la documentazione per il SuSEfirewall2.

Potrete eseguire la configurazione ricorrendo ad YaST (vd. sezione *Configurazione con YaST* a pagina 497) o direttamente nel file `/etc/sysconfig/SuSEfirewall2` che contiene delle indicazioni in lingua inglese

Configurazione manuale

Segue una guida alla configurazione passo per passo. In ogni punto, viene indicato se quanto indicato vale per il masquerading o firewall. Nel file di configurazione si parla anche di una DMZ ("Zona demilitarizzata"); ma questo non è il tema del nostro capitolo.

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): Per esempio `eth0`, il dispositivo vi porta su Internet. Nel caso di ISDN è per esempio `ipppp0`.
- FW_DEV_INT (Firewall, Masquerading): il device che punta all'interno, nella rete "privata". Se non esiste alcuna rete interna lasciate vuota questa variabile.
- FW_ROUTE (Firewall, Masquerading): se avete bisogno di masquerading, rispondete `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.

  Con 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 avete bisogno del masquerading, immettete `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 dalla rete interna.

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; per esempio `"www smtp ftp domain 443"` – per il computer "a casa" che non deve offrire alcun servizio, non inserite niente.
- FW_SERVICES_EXTERNAL_UDP (Firewall): lasciate vouto 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 quei computer di cui potete *veramente* fidarvi ("Trusted Hosts"). Tenete però a mente che anche questi computer devono venire protetti contro intrusioni. Esempio: `"172.20.0.0/16 172.30.4.2"` significa che tutti i computer, il cui indirizzo IP comincia con `172.20.x.x`, come pure il computer 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 `ssh` come servizio.
- FW_SERVICES_TRUSTED_UDP (Firewall): come sopra, solo riferito a UDP.
- FW_ALLOW_INCOMING_HIGHPORTS_TCP (Firewall): se volete lavorare con un FTP normale (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 tutti 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, su FW_TCP_SERVICES_* deve essere attivata la porta 53.

- FW_SERVICE_DHCLIENT (Firewall): se usate dhclient per ricevere il vostro indirizzo IP, impostate `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 ad Internet tramite diald o ISDN (dial on demand), impostate qui `yes`.

La configurazione così è conclusa. Non dimenticate di testare il firewall (per esempio `telnet` dall'esterno); in `/var/log/messages` dovrebbero apparire più o meno i seguenti comunicazioni:

```
Feb  7 01:54:14 www kernel: Paket log: input DENY eth0
PROTO=6 129.27.43.9:1427 195.58.178.210:23 L=60 S=0x00
I=36981 F=0x4000 T=59 SYN (#119)
```

Configurazione con YaST

Tramite il centro di controllo diYaST protrete 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 importante solo se volete offrire dei servizi tramite il vostro sistema che devono essere accessibili via Internet come server web e di posta etc. Abilitate le relative caselle e/o attivate tramite 'Per esperti ...' determinati servizi tramite il loro numero di porta (che trovate in `/etc/services`). Se il vostro computer non deve fungere da server, lasciate questo dialogo senza aver apportato alcuna modifica cliccando su 'Prossimo'.

Funzionalità Qui selezionate le principali funzionalità del vostro firewall:

- 'Permetti traceroute' per ricostrurie il routing verso il vostro firewall.
- 'Inoltra i dati ed effettua il mascheramento' protegge gli host sulla rete interna da attacchi provienti da Internet — tutti i servizi diInternet apparentemente vengono utilizzati dal vostro firewall, mentre gli host sulla 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 attivati del firewall sono accessibili per host *interni*. Dato che qui non è possibile attivare dei servizi dovreste disattivare questa opzione se intendete 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 per il vostro firewall. Prima di attivare ‘Opzioni di debug’ considerate che questi file di log o protocollo 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.

SSH – secure shell, l’alternativa sicura

Il lavoro in rete richiede l’accesso ad host remoti. L’utente deve autenticarsi tramite il proprio nome di login e password. Se questi dati non vengono cifrati possono venir intercettati da terzi e utilizzati per eseguire il login all’insaputa dell’utente. A parte il fatto che l’intrusore viola così la privacy dell’utente, può utilizzare l’accesso per sferrare ulteriori attacchi rivolti 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.

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.

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, per esempio con YaST. Potete anche indicare un nome di utente locale che differisce da quello del sistema remoto, per esempio `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 terminal locale del computer `terra`.

```
ssh sole "uptime; mkdir tmp"
password di tux@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`.

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 va ad incrementare da sinistra a destra. Inoltre, sul margine destro viene mostrato il tempo rimanente (stimato) per la trasmissione (ingl. *estimated time of arrival*). Ogni output può venire soppresso con l'opzione `-q`.

scp offre, oltre alla copia di singoli file, anche un procedimento ricorsivo per la trasmissione di complete directory: `scp -r src/ sole:backup/`

copia tutto il contenuto della directory `src/` (comprese le sottodirectory) nella sottodirectory `backup/` di `sole`. Se la sottodirectory `backup/` non esiste, viene creata automaticamente.

Per mezzo dell'opzione `-p`, scp preserva 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.

sftp - trasmissione più sicura

Alternativamente, si può usare sftp per una trasmissione dei dati più sicura. All'interno di una sessione, sftp offre molti dei comandi noti da ftp. Rispetto a scp, si rivela vantaggioso soprattutto quando si trasmettono dati di cui non si conoscono i nomi di file.

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, un server. Questi aspetta i suoi collegamenti su TCP/IP port 22.

Durante il primo avvio, il demone genera tre paia di chiavi composti 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.

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 istruzione 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, (ingl. *session key*) da lui liberamente scelta e la invia al server SSH: inoltre comunica al server il metodo di cifratura (ingl. *cipher*) usato.

Il protocollo SSH versione 2 non prevede l'uso della server key. Al suo posto viene utilizzato l'algoritmo 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. befehlman /usr/share/doc/packages/openssh/RFC.nroff). Questa fase iniziale di collegamento, può venire facilmente seguita tramite `-v`, l'opzione 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 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 l'impossibilità 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, possono essere ripristinate le vecchie chiavi eseguendo una reinstallazione. 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`.

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. Per 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 un testo lungo 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/tux/.ssh/id_rsa
Your public key has been saved in /home/tux/.ssh/id_rsa.pub.
The key fingerprint is:
79:c1:79:b2:e1:c8:20:c1:89:0f:99:94:a8:4e:da:e8 tux@sole
```

Usate `ssh-keygen -p -t rsa` o `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 su `yes` la variabile `usessh` che si trova all'inizio del file `.xsession`, ed eseguire il login tramite un display manager (p.e.KDM o XDM). Alternativamente potete usare ssh-agent startx.

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, per esempio 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`.

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 impostata `-A`, il meccanismo di autenticazione ssh-agent viene adottato 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 a "`terra` port 25", SMTP viene reindirizzato alla porta SMTP di `sole` tramite un canale cifrato. Ciò è utile specialmente per gli utenti di server SMTP senza supporto per le funzionalità SMTP-AUTH o POP-before-SMTP. Le mail possono in tal maniera venir inviati da una postazione qualsiasi con un collegamento di rete per venir consegnate dal server di posta "proprio". In modo analogo con il seguente comando le richieste POP3 (Port 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`.

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 workstation 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 punti 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

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 (ingl. *timestamp*), ovvero la datazione del file, la validità e un chiave di sessione (ingl. *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".

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 rete; limitate il più possibile i 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 ed 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 di quello 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 appena 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 secondo questa chiave che può essere decifrata dal pacchetto inviato dal server di autenticazione. Il pacchetto viene "scompattato", e sia la password che la chiave vengono cancellati dalla memoria della workstation. 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 prova (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 da lui un servizio. Queste informazioni vengono comparate a quelle contenute nel ticket. In tal il server verifica se il ticket e l'authenticator provvengono dallo stesso server.

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 all'originale TGT. 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 *Ulteriori informazioni su Kerberos* a fronte.

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, utilizzate 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/krb5-1.2/krb5-1.2.5/doc/user-guide_toc.html` di più sulle applicazioni di rete di Kerberos.

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/krb5-1.2/krb5-1.2.5/doc/user-guide_toc.html`
`http://www.lns.cornell.edu/public/COMP/krb5/install/install_toc.html`
`http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.5/doc/admin_toc.html`
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)

Installare e amministrare Kerberos

Questa sezione tratta l'installazione della implementazione Kerberos Heimdal e alcuni aspetti riguardanti l'amministrazione. Comunque, si parte dal presupposto che disponete già delle nozioni basilari in tema Kerberos (vedi anche la sezione *Autenticazione nella rete — Kerberos* a pagina 503).

Selezionare 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 di Kerberos via DNS. Per realizzare ciò, è bene che il nome del realm sia un sottodominio del vostro nome di dominio DNS.

Diversamente all'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 [Tun99].

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`.

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 a tutte le 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 effettuate 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 `!`.

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 inviati più volte ("replayed"). 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 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 *Sincronizzare l'ora* a pagina 519.

Configurazione dell'attività di log

Di default, i demoni Kerberos che girano sull'host KDC protocollanno le loro 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, eseguendo uno script di scansione dei log sull' host KDC o copiando questi file di log dal KDC su un altro host, ed analizzando 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.

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 []: <premere invio>
newbie@SAMPLE.COM's Password: <type password here>
Verifying password: <re-type password here>
```

Potete accettare i valori di default premendo (Enter). Scegliete una buona password.

Dopo generate un altro principal chiamato `newbie/admin` inserendo `add newbie/admin` al prompt di `kadmin`. Il suffisso `admin` in questo caso indica il ruolo (ingl. *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

da remoto) e kpasswd (che gestisce le richieste degli utenti di modifica della password). Per avviare il demone manualmente, inserite:

```
rckdc start
```

```
Starting kdc                done
```

Assicuratevi che il KDC venga avviato di default quando viene riavviato il server. Il comando è `insserv kdc`.

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 non immettiate indirizzi IP `krb5.conf` al posto dei nomi degli host.

La configurazione statica

Come detto, un modo per configurare Kerberos è quello di 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
```

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 cesellare 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 di `kadmin` (`man 8 kadmin`).

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`).

Generare principal di host Kerberos

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/`⟨*`nomehost`*⟩`@`⟨*`REALM`*⟩, ⟨*nomehost*⟩ 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.

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 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.

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 terra.sample.com
```

```
Last login: Fri Aug  9 14:12:50 2002 from zamboni.sample.com
Have a lot of fun...
```

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` :

```
terra:~ #  kadmin add -r ldap/mondo.sample.com
terra:~ #  ktutil get ldap/mondo.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 ((ingl. *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, per 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 rilevata 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.

La sicurezza è una questione di fiducia

Concetti fondamentali

Uno dei grandi vantaggi di un sistema Linux/Unix consiste nel fatto che diversi utenti possano svolgere le loro attività allo stesso tempo e sul medesimo sistema (multi user e multitasking). Un sistema operativo Linux/Unix è inoltre caratterizzato da un'enorme trasparenza di rete, di modo tale che gli utenti spesso non sanno se i file o le applicazioni con cui lavorano si trovano sul computer locale o nella 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 si verficava la perdita di 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.

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 fronta 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.e., dovete dimostrare all'impiegato di essere la persona alla quale è permesso l'accesso ad un determinato conto, con la vostra firma, un numero 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 farlene 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 coscienti. Accessi illeciti su computer spesso sono preceduti da una presa di contatto del tipo social engineering con il personale di una ditta, fornitiore 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 il 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 terminal seriali sono ancora diffusi, ma non vengono quasi più installati su nuove postazioni di lavoro. In relazione al tipo di accesso, il terminal 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 infrarossa). In questo caso, il cavo stesso è il punto più facile da attaccare: è sufficiente collegarvi una vecchia stampante e per registrarne la comunicazione. 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 dal luogo in cui il computer è collocato. Noi partiamo dal presupposto che il vostro computer sia ubicato in base alle vostre esigenze 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 comunque e nel caso 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.

Password

Linux non memorizza le password in chiaro ovvero non cifrate e le confronta la password immessa con quella archiviata. Altrimenti, se venisse rubato il file con tutte le password, tutti gli account del sistema ne verrebbero compromessi. Linux salva invece le password in forma criptata: ogni volta che immettete la vostra password, questa viene criptata e solo allora paragonata con quella nella memoria. Un procedimento del genere funziona solo se non è possibile evincere la password vera e propria dalla forma criptata, cosa che assicurano i cosiddetti "algoritmi a trappola", che funzionano solo in una direzione. Un aggressore che sia riuscito ad impadronirsi della password criptata 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 secondi per criptare 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

Impedite l'accesso tramite caricamento dal dischetto o dal CD-ROM smontanto i drive o impostando una password BIOS ed permettete il boot esclusivamente dal disco rigido, impostazione che va fatta nel BIOS.

Generalmente, i sistemi Linux vengono inizializzati con un boot loader che permette di inoltrare 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 impostare un'ulteriore password in `/etc/lilo.conf` per impedirlo (vedi *Boot e boot manager* a pagina 73).

Permessi di accesso

Qui vale il principio: lavorare sempre con i minori privilegi possibili. Non è assolutamente necessario leggere o scrivere una e-mail come root. Se il programma e-mail (MUA = Mail User Agent) con il quale lavorate ha un bug, questo errore avrà delle conseguenze in misura 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 dei file. Amministratori esperti e coscienziosi, quando usano il comando `ls`, aggiungono sempre l'opzione `-l` per avere un elenco dettagliato dei file assieme ai pemessi di accesso in modo da poter riconoscere subito diritti sui file 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 da `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.e. directory con accesso in scrittura per tutti (world writable) o setuser-ID-bit per file, cioè il programma non funziona con il diritto del proprietario del processo che lo ha iniziato, ma con il 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 modificazioni.

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 'Sicuerezza'. 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

Ogniqualvolta un programma elabora dei dati che stanno o stavano in un modo o nell'altro sotto la sfera di un utente, è sempre bene essere prudenti. Questa prudenza vale soprattutto per il programmatore dell'applicazione: questi deve assicurarsi che i dati vengano interpretati correttamente dal programma, che i dati non vengano scritti in parti della memoria troppo piccole e che gli sia possibile trasmettere i dati in modo consistente attraverso il proprio programma e l'interfaccia apposita.

Si ha un "buffer overflow" se, quando si scrive su un'area del buffer, non si fa attenzione alla dimensione del buffer. Potrebbe essere che i file (provenienti dall'utente) abbiano bisogno di più spazio di quello disponibile nel buffer: a causa di questo scrivere oltre ai limiti del buffer, può succedere 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 *Permessi di accesso* a fronte). 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 vale il principio dei minori diritti possibili (vd. paragrafo *Permessi di accesso* nella pagina precedente).

Poiché nei "buffer overflow" e "format string bug" esistono errori nel trattamento dei dati degli utenti, può essere che vengano sfruttati non solo se si ha già accesso ad un "login" locale: molti degli errori conosciuti, possono venire utilizzati tramite un collegamento di rete. Per questo, "buffer overflow" e "format string bug" non si lasciano classificare come attineti ai soli computer locali o alla rete.

Virus

Anche per Linux esistono i virus! I virus conosciuti sono stati scritti dai loro autori come "Proof-of-Concept", come dunque prova che il programma funziona. Ma finora non ne è ancora stato avvistato nessuno "in libertà".

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.e. il Master-Boot-Record e questo ospite deve poter venire sovrascritto dal codice del programma del virus. Grazie alle sue capacità multi user, Linux offre la possibilità di limitare l'accesso in scrittura ai file, quindi 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 che avete preso da Internet e di cui non conoscete l'origine. I pacchetti rpm della SuSE portano una firma cifrata; questa firma digitale è la garanzia per l'accuratezza con la quale 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.

I virus vanno distinti dai cosiddetti vermi che interessano la sicurezza delle reti e non richiedono un sistema ospite per proliferare.

Sicurezza nella rete

Nella sicurezza locale, si trattava di separare gli utenti *in* un computer, in particolar modo l'utente `root`. Per quando riguarda la sicurezza della rete invece l'intero sistema va protetto contro attacchi provenienti dalla rete. L'autenticazione dell'utente durante il login attraverso nome di login e password sono parte della sicurezza locale. Durante il login tramite una connessione via rete bisogna differenziare tra gli aspetti di sicurezza: fino all'autenticazione si parla di sicurezza di rete; dopo il login di sicurezza locale.

X-Windows (autenticazione X11)

Come già accennato, la trasparenza nella 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 indicato dal 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 basati sull'host e quelli basati 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 man page del comando `xhost` vi fornirà maggiori dettagli sul suo funzionamento (e contiene anche l'avviso!).

Con l'accesso di controllo basante sui "cookies" viene usata, come mezzo di riconoscimento simile ad una password, una stringa conoscuita solo dal X-servee dall'utente con login legittimo. 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 collocare una finestra sul X-server da visualizare. 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 altre finestre di nuovi X-client. Nella man page di `Xsecurity` (`man Xsecurity`) troverete più informazioni sugli aspetti di sicurezza per l'X-Windows.

`ssh` (secure shell) è in grado (tramite un collegamento rete completamente criptato) di creare in modo trasparente, cioè non direttamente visibile per l'utente, il collegamento ad un X-server: qui si parla di "X11-forwarding". Dalla parte del server, viene simulato un X-server e dalla parte della 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 (con il vostro server X, tramite il vostro collegamento ssh) anche aggressori autenticati e "origliare" alla vostra tastiera.

Attenzione

Buffer overflow e format string bugs

Quanto detto nella sezione "sicurezza locale" su "buffer overflows" e "format string" vale anche per la distinzione in locale e remoto per gli aspetti relarivi 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, vengono distribuiti i cosiddetti "exploits", programmi cioè che sfruttano lacune rilevate recentemente. Anche chi non conosca i dettagli esatti di questa lacuna, è in grado di trarne vantaggio. 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 di come eliminare il problema.

DoS - Denial of Service

L'obiettivo di questo tipo di attacco è interrompere un servizio o addirittura compromettere l'intero sistema. Ciò può succedere nei modi più disparati: tramite un sovraccarico, con attività che si occupano di pacchetti superflui o con lo sfruttamento di "remote buffer overflow", che non possono venire utilizzati direttamente per l'esecuzione di programmi sul lato remoto.

Con un attacco DoS spesso si intende fermare un servizio. La mancanza di un servizio può però avere conseguenze che vanno ben oltre. Vedi "man in the middle: sniffing, tcp connection hijacking, spoofing" e "DNS poisoning".

man in the middle: sniffing, tcp connection hijacking, spoofing

In generale, un attacco dalla rete, nel quale l'aggressore prenda posizione fra due interlocutori, viene chiamato attacco del tipo "man-in-the-middle". Spesso la vittima neanche si accorge di quello che sta accandendo. Spesso 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, poiché questi si spaccia per il computer meta. L'attacco "man in the middle" più semplice è rappresentato da uno "sniffer". Esso origlia ai collegamenti 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. *h*)ijacking) 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 vengono fatti passare davanti. Quando assume il ruolo della meta del collegamento, la vittima lo nota solo perché il collegamento viene terminato perché non valido.

L'aggressore approfitta soprattutto di quei protocolli che protetti tramite cifrati contro l'"hijacking" e nei quali all'inizio del collegamento avviene un'autenticazione. "Spoofing" viene nominato l'invio di pacchetti con i dati mittente modificati, principalmente indirizzi 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 dividere repentinamente un computer dalla rete (anche se solo per breve tempo), la cosa influenza favorvolmente un attacco attivo, poiché non si aspettano più alcuni disturbi.

DNS poisoning

L'aggressore cerca, con i pacchetti risposta DNS falsificati ("spoofed") di avvelenare (ingl. *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 creato un rapporto di fiducia verso altri computer, un tale attacco (nonostante le complicazioni) 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 della vittima, un DoS cronologicamente sintonizzato contro 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

I vermi vengono spesso comparati ai virus. Vi è tuttavia una notevole differenza: un verme non deve contagiare alcun programma ospite ed è specializzato a diffondersi rapidamente nella rete. I vermi conosciuti come Ramen, Lion o Adore utilizzano 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 disponibiltà dei pacchetti di aggiornamento. Ciò presuppone, naturalmente, che l'amministratore installi sui propri sistemi tutte le più recenti security update.

Consigli ed espedienti: indicazioni generali

Informazione: in tema di sicurezza è necessario tenere il passo con gli sviluppi nel campos 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 (avviso di sicurezza). Gli avvisi 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`. Su `http://www.securityfocus.com` troverete ancora più informazioni.

Eccovi alcune utili regole di base:

- Lavorate il meno possibile come `root`, secondo il principio: per ogni compito, servitevi dei minori privilegi possibili. Diminuirete così non solo il pericolo che si infiltrino uova di cuccù e virus o ma anche la possibilità di fare voi stessi errori irreparabili.
- Se possibile, utilizzate sempre collegamenti criptati per eseguire dei lavori in 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, può forse non essere in grado di sbrigare i suoi compiti, ma di regola 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 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 sbloccato 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 il port.

Confrontate i risultati che avete con un port scan del vostro sistema eseguito dall'esterno; a questo scopo si adatta particolarmente il programma `nmap` controllando ogni singola porta e, sulla base della risposta del vostro computer, è in grado di trarre conclusioni su un servizio in attesa dietro la porta. Non eseguite mai uno scan del vostro computer senza il permesso diretto dell'amministratore, poiché la cosa potrebbe venire scambiata per un atto di aggressione. Ricordate che dovreste eseguire uno scan non solo dei port TCP, ma anche dei port UDP (opzioni `-sS` e `-sU`).

- Per un controllo affidabile dell'integrità dei file sul vostro sistema, dovreste utilizzare `tripwire` e criptare la banca dati per proteggerla da manipolazioni. In ogni caso avete anche bisogno di un backup ovvero copia di sicurezza di questa banca dati su un supporto dati a parte a cui non è possibile accedere tramite rete.

- Fate attenzione quando installate del software. Si sono già avuti casi un cui un aggressore ha infettato archivi tar di un software di sicurezza, con 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 paket.rpm` mostra se la somma di controllo e il contrassegno del pacchetto (non installato!) coincidono. La chiave si trova sul primo CD di una distribuzione SuSE (a partire dalla versione SuSE-7.1) e sulla maggioranza dei key-server nel mondo.

- Controllate regolarmente il backup dei dati e del sistema. Senza una dichiarazione affidabile sulla funzione del backup, il backup è (eventualmente) senza valore.

- Controllate i vostri "file di log". Se possibile, scrivetevi un piccolo script che ricerchi valori strani nei vostri file di log. Questo è un compito tutt'altro che triviale, poiché solo voi potete notare avvenimenti strani 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 man `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 comuniciazione per i colleghi di lavoro.

Comunicazione centrale di 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

La chiave è disponibile anche per il download all'indirizzo `http://www.suse.de/security`.

Parte V

Appendixes

A

File system di Linux

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 vantaggi e il loro campo di impiego. 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 meta struttura. La differenza delle 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 della 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, 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 in tema 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 potete realizzare tutto comodamente con YaST, se non vengono indicati esplicitamente degli altri modi per apportare delle modifiche ai file system.

Nota

Ext2

Ext2 risale alle origini 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 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 necessita di 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 Ext2 non è particolarmente adatto per server ad alta disponibilità. Dato che Ext2 comunque non deve aggiornare 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 ad 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`.

Suggerimento

Convertire un file system Ext2 in Ext3

Convertire un file system Ext2 nel tipo Ext3 richiede i seguenti passaggi:

Creare il journal: immettete `tune2fs -j` come utente `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 pagina di manuale (`man 8 tune2fs`).

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.

Suggerimento

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 meta-dati 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 B*. 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 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

JFSil "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 la prestazione. Essendo un file system a 64 bit, JFS supporta file voluminosi e partizioni LFS (ingl. *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 B^+ 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 da 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 (ingl. *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. *to 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 a fronte 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.

`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 IBM OS/2– supportato solo nella modalità di lettura.
`iso9660`	File system standard dei CD-ROM.
`minix`	Questo file system deriva da progetti universitari riguardanti sistemi operativi ed è stato il primo file system usato sotto Linux. Oggi viene utilizzato come file system per dischetti.
`msdos`	*fat*, originariamente il file system utilizzato sotto DOS che oggi viene utilizzato da diversi sistemi operativi.
`ncpfs`	File system per montare volumi Novell tramite 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. da Windows per accedere a file tramite rete.
`sysv`	Viene utilizzato sotto SCO UNIX, Xenix e Coherent (sistemi commerciali UNIX per PC).

Tabella A.1: *Continua alla pagina seguente...*

`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 di nomi lunghi).
`vfat`	*Virtual FAT*: estensione del file system `fat` (supporta lunghi nomi di file).
`ntfs`	*Windows NT file system*, accesso in sola lettura.

Tabella A.1: *Tipi di file system sotto Linux*

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 nella pagina successiva vi offre una rassegna delle attuali restrizioni per file Linux e file system per il kernel 2.4x. .

File system	**Dim. file mass.[Byte]**	**Dim. file system mass. [Byte]**
Ext2 o Ext3 (1 kB dimensione blocco)	2^{34} (16 GB)	2^{41} (2 TB)
Ext2 o Ext3 (2 kB dimensione blocco)	2^{38} (256 GB)	2^{43} (8 TB)
Ext2 o Ext3 (4 kB dimensione blocco)	2^{41} (2 TB)	2^{44} (16 TB)
Ext2 o Ext3 (8 kB dimensione blocco) (Sistemi con page 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 dimensione blocco)	2^{63} (8 EB)	2^{49} (512 TB)
JFS (4 kB dimensione 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)

Tabella A.2: *Dimensione massima di file system (formato on-disk)*

Nota

I limiti del Linux Kernel

La tabella riporta i limiti del formato on-disk. Ecco i limiti per la dimensione massima di un file e di un file system, che può essere elaborata in modo corretto dal Kernel 2.4.x :

- *Sistemi a 32 bit:* i file e block device non possono superare i 2 TB (2^{41} byte). Comunque tramite i LVM potete combinare più block device per poter gestire file system che superano il limite di 2 TB.
- *Sistemi a 64 bit:* i file e file system possono raggiungere i 8 EB (2^{63} byte), sempre che l'hardware supporti queste dimensioni.

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/`
`http://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`.

B

Le Access Control List in Linux

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 Lists*) ed i vantaggi che ne derivano.

Perché utilizzare le ACL?

Nota

POSIX ACL

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 Linux a uno Windows 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 a cui assegnare dei 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 o registrazioni. Una registrazione ACL include il tipo (vedi la tabelle B.1 nella pagina seguente), una designazione per l'utente o il gruppo a cui si riferisce la registrazione ed dei 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.

Tipo	Forma testo
owner	`user::rwx`
named user	`user:name:rwx`
owning group	`group::rwx`
named group	`group:name:rwx`
mask	`mask::rwx`
other	`other::rwx`

Tabella B.1: *Rassegna: tipi delle registrazioni ACL*

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):

Tipo	Forma testo	Permessi
named user	`user:jane:r-x`	`r-x`
mask	`mask::rw-`	`rw-`
	permesso effettivo:	`r--`

Tabella B.2: *Mascherare i permessi di accesso*

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 nella pagina successiva e B.2 a fronte). 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:

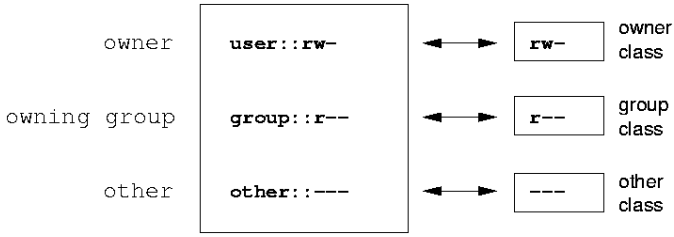


Figura B.1: *ACL minima: registrazioni ACL vs. bit dei permessi*

- Nel caso di una ACL minima — ovvero senza registrazione *mask* — i permessi *group class* vengono assegnati alla registrazione ACL *owning group* (vedi la fig. B.1).
- Nel caso di ACL estese — dunque con la registrazione *mask* — i permessi *group class* vengono assegnati alla registrazione *mask* (vd. la fig. B.2).

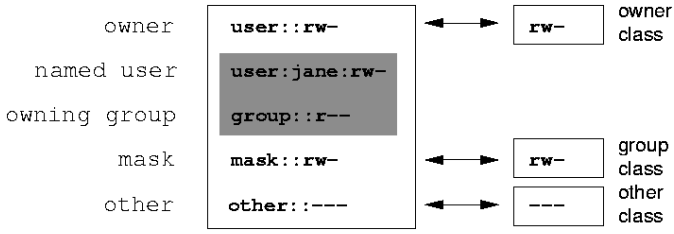


Figura B.2: *ACL estese: registrazioni ACL vs. bit dei permessi*

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 ed inversamente.

Una directory con ACL di accesso

Per poter utilizzare le ACL di accesso si dovete:

- 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 permesso 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 *Le registrazioni ACL ed i bit dei permessi* a pagina 556. 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`.

```
getfacl mydir

# 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 556). 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 (ingl. *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 *Gli effetti di una ACL di default* a pagina 561).

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".

Prospettiva

Come avete visto 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 eccezione 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 aver essere stato modificato riceve il nome del vecchio file, le ACL molto probabilmente andranno perse, almeno ché l'editor non supporti le ACL.

Quanto più esteso è il supporto per le ACL da parte delle applicazioni, tanto maggiore sarà il modo di poter sfruttare a pieno le potenzialità di questa feature.

Suggerimento

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 nella pagina di manuale di `getfacl` (`man 1 getfacl`), la pagina di manuale di `acl` (`man 5 acl`) e la pagina di manuale di `setfacl` (`man 1 setfacl`).

Suggerimento

Manual-Page di e2fsck

```
E2FSCK(8)                                                    E2FSCK(8)


NAME
       e2fsck - check a Linux second extended file system

SYNOPSIS
       e2fsck  [  -pacnyrdfvstFSV ] [ -b superblock ] [ -B block-
       size ] [ -l|-L bad_blocks_file ] [ -C fd ] [ -j  external-
       journal ] [ device

DESCRIPTION
       e2fsck  is used to check a Linux second extended file sys-
       tem (e2fs).  E2fsck also supports ext2  filesystems  coun-
       taining  a journal, which are also sometimes known as ext3
       filesystems.

       device is the special file  corresponding  to  the  device
              (e.g /dev/hdc1).

OPTIONS
       -a     This  option  does the same thing as the -p option.
              It is provided for backwards compatibility only; it
              is  suggested  that  people  use -p option whenever
              possible.

       -b superblock
              Instead of using  the  normal  superblock,  use  an
              alternative  superblock  specified  by  superblock.
              This option  is  normally  used  when  the  primary
              superblock has been corrupted.  The location of the
              backup superblock is dependent on the  filesystem's
              blocksize.   For  filesystems with 1k blocksizes, a
              backup superblock can be found at block  8193;  for
              filesystems with 2k blocksizes, at block 16384; and
              for 4k blocksizes, at block 32768.
```

Additional backup superblocks can be determined by using the mke2fs program using the -n option to print out where the superblocks were created. The -b option to mke2fs, which specifies blocksize of the filesystem must be specified in order for the superblock locations that are printed out to be accurate.

If an alternative superblock is specified and the filesystem is not opened read-only, e2fsck will make sure that the primary superblock is updated appropriately upon completion of the filesystem check.

-B blocksize
Normally, e2fsck will search for the superblock at various different block sizes in an attempt to find the appropriate block size. This search can be fooled in some cases. This option forces e2fsck to only try locating the superblock at a particular blocksize. If the superblock is not found, e2fsck will terminate with a fatal error.

-c This option causes e2fsck to run the badblocks(8) program to find any blocks which are bad on the filesystem, and then marks them as bad by adding them to the bad block inode.

-C This option causes e2fsck to write completion information to the specified file descriptor so that the progress of the filesystem check can be monitored. This option is typically used by programs which are running e2fsck. If the file descriptor specified is 0, e2fsck will print a completion bar as it goes about its business. This requires that e2fsck is running on a video console or terminal.

-d Print debugging output (useless unless you are debugging e2fsck).

-f Force checking even if the file system seems clean.

-F Flush the filesystem device’s buffer caches before beginning. Only really useful for doing e2fsck time trials.

-j external-journal
Set the pathname where the external-journal for this filesystem can be found.

-l filename
Add the blocks listed in the file specified by filename to the list of bad blocks. The format of this file is the same as the one generated by the badblocks(8) program.

-L filename
Set the bad blocks list to be the list of blocks specified by filename. (This option is the same as the -l option, except the bad blocks list is cleared before the blocks listed in the file are added to the bad blocks list.)

-n Open the filesystem read-only, and assume an answer of 'no' to all questions. Allows e2fsck to be used non-interactively. (Note: if the -c, -l, or -L options are specified in addition to the -n option, then the filesystem will be opened read-write, to permit the bad-blocks list to be updated. However, no other changes will be made to the filesystem.)

-p Automatically repair ("preen") the file system without any questions.

-r This option does nothing at all; it is provided only for backwards compatibility.

-s This option will byte-swap the filesystem so that it is using the normalized, standard byte-order (which is i386 or little endian). If the filesystem is already in the standard byte-order, e2fsck will take no action.

-S This option will byte-swap the filesystem, regardless of its current byte-order.

-t Print timing statistics for e2fsck. If this option is used twice, additional timing statistics are printed on a pass by pass basis.

-v Verbose mode.

-V Print version information and exit.

-y Assume an answer of 'yes' to all questions; allows e2fsck to be used non-interactively.

EXIT CODE

The exit code returned by e2fsck is the sum of the following conditions:

```
0    - No errors
1    - File system errors corrected
2    - File system errors corrected, system should
       be rebooted if file system was mounted
4    - File system errors left uncorrected
8    - Operational error
16   - Usage or syntax error
128  - Shared library error
```

SIGNALS

The following signals have the following effect when sent to e2fsck.

SIGUSR1

This signal causes e2fsck to start displaying a completion bar. (See discussion of the -C option.)

SIGUSR2

This signal causes e2fsck to stop displaying a completion bar.

REPORTING BUGS

Almost any piece of software will have bugs. If you manage to find a filesystem which causes e2fsck to crash, or which e2fsck is unable to repair, please report it to the author.

Please include as much information as possible in your bug report. Ideally, include a complete transcript of the e2fsck run, so I can see exactly what error messages are displayed. If you have a writeable filesystem where the transcript can be stored, the script(1) program is a handy way to save the output of e2fsck to a file.

It is also useful to send the output of dumpe2fs(8). If a specific inode or inodes seems to be giving e2fsck trouble, try running the debugfs(8) command and send the output of the stat(1u) command run on the relevant inode(s). If the inode is a directory, the debugfs dump command will allow you to extract the contents of the directory inode, which can sent to me after being first run through uuencode(1).

Always include the full version string which e2fsck displays when it is run, so I know which version you are running.

```
AUTHOR
       This  version  of  e2fsck  was  written  by  Theodore Ts'o
       <tytso@mit.edu>.

SEE ALSO
       mke2fs(8), tune2fs(8), dumpe2fs(8), debugfs(8)


E2fsprogs version 1.25    September 2001                E2FSCK(8)
```

Manual-Page di reiserfsck

```
REISERFSCK(8)                                        REISERFSCK(8)


NAME
       reiserfsck - check a Linux Reiserfs file system

SYNOPSIS
       reiserfsck  [  -afprVy  ]  [  --check  |  --fix-fixable  |
       --rebuild-sb | --rebuild-tree | --clean-attributes ] [  -j
       |  --journal-device  device ] [ --no-journal-available ] [
       -z | --adjust-file-size ] [ -S | --scan-whole-partition  ]
       [  -l  |  --logfile  filename  ]  [  -n | --nolog ] [ -q |
       --quiet ] device

DESCRIPTION
       Reiserfsck searches for a Reiserfs filesystem on a device,
       replays  any  necessary transactions, and either checks or
       repairs the file system.

       device is the special file corresponding to the device  or
              partition  (e.g /dev/hdXX for IDE disk partition or
              /dev/sdXX for SCSI disk partition).

OPTIONS
       --check
              This default action checks file system  consistency
              and reports but does not repair any corruption that
              it finds. This option may be used  on  a  read-only
              file  system  mount.  The --check option exits with
              status 0 to indicate that no corruption was  found.
              Otherwise, reiserfsck returns 1 to indicate corrup
              tion that can be fixed with --fix-fixable and 2  to
              indicate corruption that requires --rebuild-tree.

       --fix-fixable
              This  option  recovers  certain kinds of corruption
```

that do not require rebuilding the entire file sys tem tree (--rebuild-tree). Normally you only need this option if the --check option reports "corrup tion that can be fixed with --fix-fixable". This includes: zeroing invalid data-block pointers, cor recting st_size and st_blocks for directories, and deleting invalid directory entries.

--rebuild-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.

--rebuild-tree
This option rebuilds the entire file system tree using leaf nodes found on the device. Normally you only need this option if the --check option reports "corruption that can be fixed only during --rebuild-tree". You are strongly encouraged to make a backup copy of the whole partition before attempting the --rebuild-tree option.

--clean-attributes
This option cleans reserved fields of Stat-Data items.

--journal-device device , -j device
This option supplies the device name of the current file system journal. This option is required when the journal resides on a separate device from the main data device (although it can be avoided with the expert option --no-journal-available).

--adjust-file-size, -z
This option causes reiserfsck to correct file sizes that are larger than the offset of the last discov ered byte. This implies that holes at the end of a file will be removed. File sizes that are smaller than the offset of the last discovered byte are corrected by --fix-fixable.

--logfile filename, -l filename
This option causes reiserfsck to report any corrup tion it finds to the specified log file rather than stderr.

--nolog, -n
This option prevents reiserfsck from reporting any kinds of corruption.

--quiet, -q

```
            This  option prevents reiserfsck from reporting its
            rate of progress.

        -a, -p These options are usually passed by fsck -A  during
            the  automatic  checking  of /etc/fstab partitions.
            For compatibility, these options simply cause reis
            erfsck  to  print  information  about the specified
            file system.  No checks are performed.  When it  is
            set  - reiserfsck assumes that it is called by fsck
            -A, provides some information about  the  specified
            filesystem and exits.

        -V     This  option  prints  the reiserfsprogs version and
            exit.

        -r, -p, -y
            These options are ignored.

        -V, -f prints version and exits

EXPERT OPTIONS
        DO NOT USE THESE OPTIONS UNLESS  YOU  KNOW  WHAT  YOU  ARE
        DOING.   WE  ARE  NOT  RESPONSIBLE  IF  YOU LOSE DATA AS A
        RESULT OF THESE OPTIONS.

        --no-journal-available
            This option allows reiserfsck to proceed  when  the
            journal device is not available. This option has no
            effect when the journal is located on the main data
            device.  NOTE:  after  this  operation you must use
            reiserfstune to specify a new journal device.

        --scan-whole-partition, -S
            This option causes --rebuild-tree to scan the whole
            partition, not only used space on the partition.

EXAMPLE OF USING
        1. You think something may be wrong with a reiserfs 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 CODE

reiserfsck uses the following exit codes:

```
0      - No errors
1      - File system errors corrected
2      - File system errors corrected, system should
         be rebooted if file system was mounted
4      - File system errors left uncorrected
8      - Operational error
16     - Usage or syntax error
```

AUTHOR

This version of reiserfsck has been written by Vitaly Fertman <vitaly@namesys.com> and Vladimir Saveliev <vs@namesys.com>.

BUGS

There are likely to be some bugs. Please report bugs to the ReiserFS mail-list <reiserfs-list@namesys.com>.

TODO

Faster recovering, signal handling, i/o error handling, return reasonable exit codes, etc.

SEE ALSO

mkreiserfs(8), debugreiserfs(8), reiserfstune(8)

Reiserfsprogs-3.6.2 January 2002 REISERFSCK(8)

La Licenza Pubblica GNU (GPL)

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 usa la licenza GPL. Solo la versione originale in inglese della licenza ha valore legale. Ad ogni modo, speriamo che questa traduzione aiuti le persone di lingua italiano a capire meglio il significato della licenza GPL.

This is an unofficial translation of the GNU General Public License into Italian. It was not published by the Free Software Foundation, and does not legally state the distribution terms for software that uses the GNU GPL–only the original English text of the GNU GPL does that. However, we hope that this translation will help Italian speakers understand the GNU GPL better.

LICENZA PUBBLICA GENERICA (GPL) DEL PROGETTO GNU
Versione 2, Giugno 1991

Traduzione curata dal gruppo Pluto e da
ILS, ultimo aggiornamento, 30 luglio 1998.

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 "free software", ci si sriferisce alla libertà, non al prezzo. Le nostre Licenze (la GPL e la LGPL) sono progettate per assicurarsi che ciascuno 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 è coperto 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.

   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.

2. 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:

   (a) Bisogna indicare chiaramente nei file che si tratta di copie modificate e la data di ogni modifica.

   (b) 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.

(c) 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:

   (a) 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.

   (b) 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.

(c) 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 B. @end enumerate

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 all'acquirente nel suo esercizio dei diritti qui garantiti. Chi distribuisce programmi coperti da questa Licenza non e' comunque responsabile per la conformità alla Licenza da parte di terze parti.

7. Se, come conseguenza del giudizio di una corte, o di una imputazione per la violazione di un brevetto o per ogni altra ragione (anche non relativa a questioni di brevetti), vengono imposte condizioni che contraddicono le condizioni di questa licenza, che queste condizioni siano dettate dalla corte, da accordi tra le parti o altro, queste condizioni non esimono nessuno dall'osservazione di questa Licenza. Se non è possibile distribuire un prodotto in un modo che soddisfi simultaneamente gli obblighi dettati da questa Licenza e altri obblighi pertinenti, il prodotto non può essere affatto distribuito. Per esempio, se un brevetto non permettesse a tutti quelli che lo ricevono di ridistribuire il Programma senza obbligare al pagamento di diritti, allora l'unico modo per soddisfare contemporaneamente il brevetto e questa Licenza e' di non distribuire affatto il Programma.

   Se parti di questo punto sono ritenute non valide o inapplicabili per qualsiasi circostanza, deve comunque essere applicata l'idea espressa da questo punto; in ogni altra circostanza invece deve essere applicato il punto 7 nel suo complesso.

   Non è nello scopo di questo punto indurre gli utenti ad infrangere alcun brevetto nè ogni altra rivendicazione di diritti di proprietà, nè di contestare la validità di alcuna di queste rivendicazioni; lo scopo di questo punto è solo quello di proteggere l'integrità del sistema di distribuzione dei programmi liberi, che viene realizzato tramite l'uso della licenza pubblica. Molte persone hanno contribuito generosamente alla vasta gamma di programmi distribuiti attraverso questo sistema, basandosi sull'applicazione fedele di tale sistema. L'autore/donatore può decidere di sua volontà se preferisce distribuire il software avvalendosi di altri sistemi, e l'acquirente non può imporre la scelta del sistema di distribuzione.

   Questo punto serve a rendere il più chiaro possibile ciò che crediamo sia una conseguenza del resto di questa Licenza.

8. Se in alcuni paesi la distribuzione e/o l'uso del Programma sono limitati da brevetto o dall'uso di interfacce coperte da copyright, il detentore del copyright originale che pone il Programma sotto questa Licenza può aggiungere limiti geografici espliciti alla distribuzione, per escludere questi

paesi dalla distribuzione stessa, in modo che il programma possa essere distribuito solo nei paesi non esclusi da questa regola. In questo caso i limiti geografici sono inclusi in questa Licenza e ne fanno parte a tutti gli effetti.

9. All'occorrenza la Free Software Foundation può pubblicare revisioni o nuove versioni di questa Licenza Pubblica Generica. Tali nuove versioni saranno simili a questa nello spirito, ma potranno differire nei dettagli al fine di coprire nuovi problemi e nuove situazioni.

   Ad ogni versione viene dato un numero identificativo. Se il Programma asserisce di essere coperto da una particolare versione di questa Licenza e "da ogni versione successiva", 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.

‹una riga per dire in breve il nome del programma e cosa fa›
Copyright (C) 19aa
‹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., 675 Mass Ave, Cambridge, MA 02139, Stati Uniti. 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:

Orcaloca versione 69, Copyright (C) 19aa <nome dell'autore> Orcaloca 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 g" e "show c" mostreranno le parti appropriate della Licenza Pubblica Generica. Chiaramente, i comandi usati possono essere chiamati diversamente da "show g" e "show c" e 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:

Yoyodinamica SPA rinuncia con questo documento ad ogni interesse al copyright del programma 'Orcaloca' (che svolge dei passi di compilazione) scritto da Giovanni Smanettone.

‹firma di Primo Tizio›, 1 April 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

[Alm96] ALMESBERGER, Werner: *LILO User's guide*, 1996. – (siehe Datei `/usr/share/doc/lilo/user.dvi`)

[Bai97] BAILEY, Edward C.: *Maximum RPM*. Red Hat, 1997. – (ISBN 1-888172-78-9)

[BBD+97] BECK, Michael; BÖHME, Harald; DZIADZKA, Mirko; KUNITZ, Ulrich; MAGNUS, Robert ; VERWORNER, Dirk: *Linux-Kernel-Programmierung*. 4. Aufl. Addison Wesley GmbH, 1997. – (ISBN 3-8273-1144-6)

[BD98] BORKNER-DELCARLO, Olaf: *Linux im kommerziellen Einsatz*. Carl Hanser Verlag, 1998. – (ISBN 3-446-19465-7)

[BD99] BORKNER-DELCARLO, Olaf: *Das Samba-Buch*. SuSE PRESS, 1999. – (ISBN 3-930419-93-9)

[CAR93] COSTALES, Bryan; ALLMAN, Eric ; RICKERT, Neil: *sendmail*. O'Reilly & Associates, Inc., 1993. – (ISBN 1-56592-056-2)

[CB96] CHESWICK, William R.; BELLOVIN, Steven M.: *Firewalls und Sicherheit im Internet*. Addison Wesley GmbH, 1996. – (ISBN 3-89319-875-x)

[CZ96] CHAPMAN, Brent; ZWICKY, Elisabeth D.: *Einrichten von Internet Firewalls. Sicherheit im Internet gewährleisten.*. O'Reilly & Associates, Inc., 1996. – (ISBN 3-930673312)

[DR99] DAWSON, Terry; RUBINI, Alessandro: *NET3-4 HOWTO*, v1.5, August 1999. – (siehe Datei `/usr/share/doc/howto/en/NET3-4-HOWTO.gz`)

[EH98] ECKEL, George; HARE, Chris: *Linux – Internet Server*. Carl Hanser Verlag, 1998. – (ISBN 3-446-19044-9)

[FCR93] FANG, Chin; CROSSON, Bob ; RAYMOND, Eric S.: *The Hitchhiker's Guide to X386/XFree86 Video Timing (or, Tweaking your Monitor for Fun and Profit)*, 1993. – (siehe Datei `/usr/X11/lib/X11/doc/VideoModes.doc`)

[Fis00] FISCHER, Thorsten: *GUI-Programmierung mit GTK+ (Handbuch und Referenz)*. SuSE PRESS, 2000. – ISBN (3–934678–42–4)

[Fri93] FRISCH, Æleen: *Essential System Administration*. O'Reilly & Associates, Inc., 1993. – (ISBN 0-937175-80-3)

[Gil92] GILLY, Daniel: *UNIX in a nutshell: System V Edition*. O'Reilly & Associates, Inc., 1992. – (ISBN 1-56592-001-5)

[GMR97] GOOSSENS, Michel; MITTELBACH, Frank ; RAHTZ, Sebastian: *The LaTeX Graphics Companion*. Addison Wesley Longman, 1997. – (ISBN 0-201-85469-4)

[GMS94] GOOSSENS, Michel; MITTELBACH, Frank ; SAMARIN, Alexander: *The LaTeX Companion*. Addison Wesley GmbH, 1994. – (ISBN 0-201-54199-8)

[GMS96] GOOSSENS, Michel; MITTELBACH, Frank ; SAMARIN, Alexander: *Der LaTeX-Begleiter*. Addison Wesley GmbH, 1996. – (ISBN 3-89319-646-3)

[GR99] GOOSSENS, Michel; RAHTZ, Sebastian: *The LaTeX Web Companion*. Addison Wesley Longman, 1999. – (ISBN 0-201-43322-7)

[GS93] GARFINKEL, Simson; SPAFFORD, Gene: *Practical UNIX Security*. O'Reilly & Associates, Inc., 1993. – (ISBN 0-937175-72-2)

[Hei96] HEIN, Jochen: *Linux-Companion zur Systemadministration*. Addison Wesley GmbH, 1996. – (ISBN 3-89319-869-5)

[Her92] HEROLD, H.: *UNIX Grundlagen*. Addison Wesley GmbH, 1992. – (ISBN 3-89319-542-8)

[HHMK96] HETZE, Sebastian; HOHNDEL, Dirk; MÜLLER, Martin ; KIRCH, Olaf: *Linux Anwenderhandbuch*. 6. Aufl. LunetIX Softfair, 1996. – (ISBN 3-929764-05-9)

[Hof97] HOFFMANN, Erwin: EMail-Gateway mit qmail. In: *iX* 12 (1997), S. 108ff.

[HR98] HÖLZER, Matthias; RÖHRIG, Bernhard: *KDE – Das K Desktop Environment*. Computer & Literatur, 1998. – (ISBN 3-932311-50-7)

[Hun95] HUNT, Craig: *TCP/IP Netzwerk Administration*. O'Reilly & Associates, Inc., 1995. – (ISBN 3-930673-02-9)

[JT98] JOHNSON, Michael K.; TROAN, Erik W.: *Anwendungen entwickeln unter Linux*. Addison Wesley GmbH, 1998. – (ISBN 3-8273-1449-6)

[Kie95] KIENLE, Micheal: TIS: Toolkit für anwendungsorientierte Firewall-Systeme. In: *iX* 8 (1995), S. 140ff.

[Kir95] KIRCH, Olaf: *LINUX Network Administrator's Guide*. O'Reilly & Associates, Inc., 1995. – (ISBN 1-56592-087-2)

[Kof99] KOFLER, Michael: *Linux – Installation, Konfiguration, Anwendung*. 4. Aufl. Addison Wesley GmbH, 1999. – (ISBN 3-8273-1475-5)

[Kop94] KOPKA, Helmut: *LaTeX-Einführung*. Addison Wesley GmbH, 1994. – (ISBN 3-89319-664-1)

[Kopff] KOPKA, Helmut: *LaTeX*. Addison Wesley GmbH, 1996 ff. – 3 Bde. (ISBN 3-8273-1025-3; 3-8273-1229-9; 3-89319-666-8)

[Kun95] KUNITZ, Ulrich: Sicherheit fast kostenlos: Einrichtung eines kostenlosen Firewall-Systems. In: *iX* 9 (1995), S. 176ff.

[Lam90] LAMB, Linda: *Learning the vi Editor*. O'Reilly & Associates, Inc., 1990. – (ISBN 0-937175-67-6)

[Lef96] LEFFLER, Sam: *HylaFAX Home Page*, 1996

[Meg98] MEGGINSON, David: *Structuring XML Documents*. Prentice-Hall, 1998. – ISBN (0–13–642299–3)

[Moh98] MOHR, James: *UNIX-Windows-Integration*. International Thomson Publishing, 1998. – (ISBN 3-8266-4032-2)

[OT92] O'REILLY, Tim; TODINO, Grace: *Managing UUCP and Usenet*. O'Reilly & Associates, Inc., 1992. – (ISBN 0-937175-93-5)

[POL97] PEEK, Jerry; O'REILLY, Tim ; LOUKIDES, Mike: *Unix Power Tools*. 2. Aufl. Sebastopol : O'Reilly & Associates, Inc., 1997

[Rub98] RUBINI, Alessandro: *Linux-Gerätetreiber*. O'Reilly & Associates, Inc., 1998. – (ISBN 3-89721-122-X)

[Sch98] SCHEIDERER, Jürgen: Sicherheit Kostenlos - Firewall mit Linux. In: *iX* 12 (1998)

[Sto98] STOLL, Clifford: *Kuckucksei. Die Jagd auf die deutschen Hacker, die das Pentagon knackten*. Fischer-TB.-Vlg., 1998. – (ISBN 3596139848)

[SuS03] SUSE LINUX AG: *SuSE Linux.*. 2. Nürnberg : SuSE Linux AG, 2003

[The96] THE XFREE86™-TEAM: *XF86Config(4/5) – Configuration File for Xfree86™*, 1996. – Manual-Page zu XFree86™

[TSP93] TODINO, Grace; STRANG, John ; PEEK, Jerry: *Learning the UNIX operating system*. O'Reilly & Associates, Inc., 1993. – (ISBN 1-56592-060-0)

[Tun99] TUNG, Brian: *Kerberos: A Network Authentication System*. Fischer-TB.-Vlg., 1999. – (ISBN 0-201-37924-4)

[Wel94] WELSH, Matt: *Linux Installation and Getting Started*. 2. Aulf. SuSE GmbH, 1994. – (ISBN 3-930419-03-3)

[WK95] WELSH, Matt; KAUFMAN, Lars: *Running Linux*. O'Reilly & Associates, Inc., 1995. – (ISBN 1-56592-100-3)

[WK98] WELSH, Matt; KAUFMAN, Lars: *Linux – Wegweiser zur Installation & Konfiguration*. 2. Aufl. O'Reilly & Associates, Inc., 1998. – (ISBN 3-930673-58-4)

[WM99] WALSH, Norman; MUELLNER, Leonard: *DocBook. The Definiteve Guide*. O'Reilly & Associates, Inc., 1999. – ISBN (1–56592–580–7)

Indice analitico

D

E

F

G

H

I

J

K

L

R

S

T

U

V

W

X

Y